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

(21) BR 112019008036-8 A2

(22) Data do Depósito: 27/11/2018

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

(54) Título: SISTEMAS, MEIOS DE ARMAZENAMENTO E MÉTODOS PARA PROTEÇÃO DE INFORMAÇÕES

(51) Int. Cl.: G06Q 40/04.

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

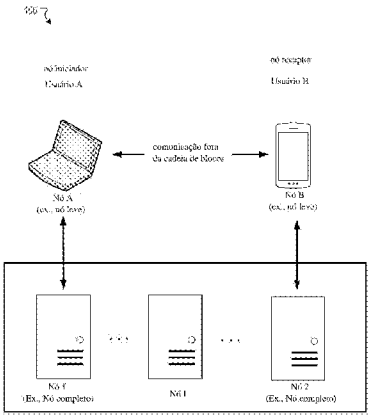
(72) Inventor(es): HUANYU MA; WENBIN ZHANG; BAOLI MA; ZHENG LIU; JIAHUI CUI.

(86) Pedido PCT: PCT CN2018117558 de 27/11/2018

(87) Publicação PCT: WO 2019/072277 de 18/04/2019

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

(57) Resumo: Um método implementado por computador para proteção de informações compreende: comprometer um valor de transação de uma transação com um primei-ro esquema de compromisso para obter um valor de compromisso de transação, comprometer uma alteração da transação com um segundo esquema de compro-misso para obter um valor de compromisso de alteração, o primeiro esquema de compromisso compreendendo um fator de ocultação de transação, e o segundo es-quema de compromisso compreendendo um fator de ocultação de alteração; cripto-grafar uma primeira combinação do fator de ocultação de alteração e a alteração com uma primeira chave; transmitir o fator de ocultação de transação, o valor de transação, e o valor de compromisso de transação para um nó receptor associado a um receptor para o nó receptor verificar a transação; em resposta a isso, o receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocultação de transação e da quantidade de transação criptografada com uma segunda chave.



“SISTEMAS, MEIOS DE ARMAZENAMENTO E MÉTODOS PARA PROTEÇÃO DE INFORMAÇÕES”

CAMPO TÉCNICO

[001]A presente divulgação geralmente se refere a métodos e dispositivos para proteção de informações.

ANTECEDENTES

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

SUMÁRIO

[003]Várias modalidades da presente divulgação incluem sistemas, métodos e meios legíveis por computador não transitórios para proteção de informações.

[004]De acordo com um aspecto, uma método implementado por computador para proteção de informações compreende: comprometer um valor de transação t de uma transação com um primeiro esquema de compromisso para obter um valor de compromisso de transação T, e comprometer uma alteração y da transação com um segundo esquema de compromisso para obter um valor de alteração compromisso Y, o primeiro esquema de compromisso compreendendo um fator de ocultação de transação r_t, e o segundo esquema de compromisso compreendendo um fator de ocultação de alteração r_y; criptografar uma primeira combinação do fator de ocultação de alteração r_y e a alteração y com uma primeira chave KA; transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de compromisso de transação T para um nó receptor associado a um receptor de transação para o nó receptor verificar a transação; em resposta ao fato de que o nó receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocul-

tação de transação r_t e o valor de transação t criptografado com uma segunda chave KB; e transmitir a primeira combinação criptografada e a segunda combinação criptografada para uma pluralidade de nós em uma blockchain para os nós na blockchain para verificar a transação.

[005]Em algumas modalidades, o primeiro esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator de ocultação de transação r_t e com o valor de transação t sendo um valor de compromisso correspondente; e o segundo esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator de ocultação de alteração r_y e com a alteração y sendo um valor de compromisso correspondente.

[006]Em algumas modalidades, transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de compromisso de transação T para o nó receptor associado ao receptor de transação para o nó receptor verificar se a transação compreende: transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de compromisso de transação T para o nó receptor associado ao receptor de transação, fazer com que o nó receptor verifique se o valor de compromisso de transação T é igual ao primeiro esquema de compromisso comprometendo o valor de transação t com o fator de ocultação de transação r_t.

[007]Em algumas modalidades, obter a segunda combinação criptografada compreende receber do nó receptor a segunda combinação criptografada e uma assinatura SIGB associada à segunda combinação criptografada e ao valor de compromisso de transação T.

[008]Em algumas modalidades, o valor de transação t é explorado de um ou mais ativos A_1, A_2,..., A_k de um emissor da transação; cada um dos ativos está associado a (1) um compromisso de Pedersen com base pelo menos em um fator de ocultação r_{ak} e um valor de cada ativo e (2) uma criptografia com base pelo menos no fator de ocultação r_{ak} e no valor de cada de ativos; e a alteração y é uma diferen-

ça entre o valor de transação t e os ativos explorados.

[009]Em algumas modalidades, antes de transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós na blockchain, o método compreende ainda: verificar a assinatura SIGB; e em resposta à verificação bem-sucedida da assinatura SIGB, gerar uma assinatura SIGA associada aos ativos A_1, A_2,..., A_k, a primeira combinação, a segunda combinação, o valor de compromisso de transação T, o valor de compromisso de alteração Y e uma diferença entre uma soma de fatores de ocultação correspondentes aos ativos A_1, A_2,..., A_k e uma soma do fator de ocultação de transação r_t e do fator de ocultação de alteração r_y.

[010]Em algumas modalidades, a transmissão da primeira combinação criptografada e da segunda combinação criptografada para a pluralidade de nós na blockchain compreende: transmitir os ativos A_1, A_2,..., A_k, a primeira combinação, a segunda combinação, o valor de compromisso de transação T, o valor de compromisso de alteração Y, uma diferença entre uma soma de fatores de ocultação correspondentes aos ativos A_1, A_2,..., A_k e uma soma do fator de ocultação de transação r_t e o fator de ocultação de alteração r_y, a assinatura SIGA, e a assinatura SIGB para a pluralidade de nós na blockchain.

[011]Em algumas modalidades, a transmissão da primeira combinação criptografada e da segunda combinação criptografada para a pluralidade de nós em uma blockchain para os nós na blockchain para verificar a transação compreende: transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós em uma blockchain, fazer com que os nós na blockchain, em resposta à verificação bem-sucedida da transação, emitam o valor de transação t para o receptor, eliminem os ativos A_1, A_2,..., A_k e emitam a alteração y para o emissor.

[012]De acordo com outro aspecto, um meio de armazenamento legível por

computador não transitório armazena instruções que, quando executadas por um processador, fazem com que o processador realize operações que incluem: comprometer um valor de transação t de uma transação com um primeiro esquema de compromisso para obter um compromisso de transação valor de T, e comprometer uma alteração y da transação com um segundo esquema de compromisso para obter um valor de alteração compromisso Y, o primeiro esquema de compromisso compreendendo um fator de ocultação de transação r_t, e o segundo esquema de compromisso compreendendo um fator de ocultação de alteração $r_{y;;}$ criptografar uma primeira combinação do fator de ocultação de alteração r_y e a alteração y com uma primeira chave KA; transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de compromisso de transação T para um nó receptor associado a um receptor de transação para o nó receptor verificar a transação; em resposta ao fato de que o nó receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocultação de transação r_t e do valor de transação t criptografado com uma segunda chave KB; e transmitir a primeira combinação criptografada e a segunda combinação criptografada para uma pluralidade de nós em uma blockchain para os nós na blockchain para verificar a transação.

[013]De acordo com um outro aspecto, um sistema para proteção de informações compreende um processador e um meio de armazenamento legível por computador não transitório acoplado ao processador, o meio de armazenamento armazenando instruções que, quando executadas pelo processador, fazer com que o sistema realize operações que compreendem: comprometer um valor de transação t de uma transação com um primeiro esquema de compromisso para obter um valor de compromisso de transação T, e comprometer uma alteração y da transação com um segundo esquema de compromisso para obter um valor de compromisso de alteração Y, o primeiro esquema de compromisso compreendendo um fator de ocultação de r_t, e o segundo esquema de compromisso compreendendo um fator de ocul-

tação de alteração r_y; criptografar uma primeira combinação do fator de ocultação de alteração r_y e a alteração y com uma primeira chave KA; transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de compromisso de transação T para um nó receptor associado a um receptor de transação para o nó receptor verificar a transação; em resposta ao fato de que o nó receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocultação de transação r_t e o valor de transação t criptografado com uma segunda chave KB; e transmitir a primeira combinação criptografada e a segunda combinação criptografada para uma pluralidade de nós em uma blockchain para os nós na blockchain para verificar a transação.

[014]De acordo com outro aspecto, um método implementado por computador para obter proteção de informações compreende: obter uma transação de ocultação fator r_t, um valor de transação t de uma transação, e um valor de compromisso de transação T de um nó emissor associado a um emissor de uma transação, em que: o valor de transação t é comprometido com um primeiro esquema de compromisso para obter o valor de compromisso de transação T, o primeiro esquema de compromisso compreendendo o fator de ocultação de transação r_t; verificar a transação com base no fator de obtenção de transação obtido r_t, no valor de transação obtido t de uma transação, e no valor de compromisso de transação T obtido; em resposta à verificação com sucesso da transação, criptografar uma segunda combinação do fator de ocultação de transação r_t e do valor de transação t com uma segunda chave KB; e transmitir a segunda combinação criptografada ao nó emissor.

[015]Em algumas modalidades, verificar a transação com base no fator de ocultação de transação r_t obtido, no valor de transação t obtido de uma transação e no valor de compromisso de transação obtido T compreende verificar se o valor do compromisso da transação T obtido é igual ao primeiro esquema de compromisso que compromete o valor de transação t obtido com o fator de ocultação de transação

r_t obtido.

[016]Em algumas modalidades, antes de transmitir a segunda combinação criptografada ao nó emissor, compreendendo ainda gerar uma assinatura SIGB associada com a segunda combinação criptografada e o valor de compromisso da transação T; e transmitir a segunda combinação criptografada para o nó emissor compreende transmitir a segunda combinação criptografada e a assinatura SIGB ao nó emissor.

[017]De acordo com outro aspecto, um meio de armazenamento legível por computador não transitório, armazena instruções que, quando executadas por um processador, fazem com que o processador execute operações compreendendo: obter um fator de ocultação de transação r_t, um valor de transação t de uma transação, e um valor de compromisso de transação T de um nó emissor associado a um emissor de uma transação, em que: o valor de transação t é comprometido com um primeiro esquema de compromisso para obter o valor de compromisso de transação T, o primeiro esquema de compromisso compreendendo o fator de ocultação de transação r_t; verificar a transação com base no fator de ocultação de transação r_t obtido, no valor de transação t obtido de uma transação e no valor de compromisso de transação obtido T; em resposta à verificação com sucesso da transação, criptografar uma segunda combinação do fator de ocultação de transação r_t e do valor de transação t com uma segunda chave KB; e transmitir a segunda combinação criptografada para o nó emissor.

[018]De acordo com um outro aspecto, um sistema para proteção de informações compreende um processador e um meio de armazenamento legível por computador não transitório acoplado ao processador, o meio de armazenamento armazenando instruções que, quando executadas pelo processador, fazem com que o sistema realize operações que compreendem: obter um fator de ocultação de transação r_t, um valor de transação t de uma transação e um valor de compromisso de

transação T de um nó emissor associado a um emissor de uma transação, em que: o valor de transação t é comprometido com um primeiro esquema de compromisso para obter o valor de compromisso de transação T, o primeiro esquema de compromisso compreendendo o fator de ocultação de transação r_t; verificar a transação com base no fator de ocultação de transação r_t obtido, no valor de transação t obtido de uma transação e no valor de compromisso de transação obtido T; em resposta à verificação com sucesso da transação, criptografar uma segunda combinação do fator de ocultação de transação r_t e do valor de transação t com uma segunda chave KB; e transmitir a segunda combinação criptografada para o nó emissor.

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

BREVE DESCRIÇÃO DOS DESENHOS

[020]Determinadas características das várias modalidades da presente tecnologia são apresentadas com particularidade nas reivindicações anexas. Uma melhor compreensão das características e vantagens da tecnologia será obtida por referência à seguinte descrição detalhada que apresenta modalidades ilustrativas, nas quais os princípios da invenção são usados, e os desenhos anexos dos quais:

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

[022]A FIG. 2 ilustra etapas exemplificadoras para iniciação e verificação de

transações, de acordo com várias modalidades.

[023]A FIG. 3 ilustra um fluxograma de um método exemplificador para proteção de informações, de acordo com várias modalidades.

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

[025]A FIG. 5 ilustra um diagrama de blocos de um sistema de computador exemplificador no qual qualquer uma das modalidades aqui descritas pode ser implementada.

DESCRIÇÃO DETALHADA

[026]A blockchain pode ser considerada como um banco de dados descentralizado, comumente referido como um ledger distribuído porque a transação é executada por vários nós (por exemplo, dispositivos de computação) em uma rede. Qualquer informação pode ser escrita na blockchain e salva ou lida a partir dela. Qualquer um pode configurar um servidor e ingressar na rede de blockchain para se tornar um nó. Qualquer nó pode contribuir com potência de computação para manter a blockchain executando cálculos complexos, como o cálculo de hash para adicionar um bloco a uma blockchain atual, e o bloco adicionado pode conter vários tipos de dados ou informações. O nó que contribuiu com a potência de computação para o bloco adicionado pode ser recompensado com um token (por exemplo, unidade monetária digital). Como a blockchain não possui um nó central, cada nó é igual e contém todo o banco de dados da blockchain.

[027]Os nós são, por exemplo, dispositivos de computação ou grandes sistemas de computador que suportam a rede de blockchain e a mantém funcionando facilmente. Existem dois tipos de nós, nós completos e nós leves. Os nós completos mantêm uma cópia completa da blockchain. Os nós completos na rede de blockchain validam as transações e os blocos que eles recebem e os retransmitem a pares conectados para fornecer verificação consensual das transações. Os nós leves,

por outro lado, baixam apenas uma fração da blockchain. Por exemplo, os nós leves são usados para transações em moeda digital. Um nó leve se comunicará com um nó completo quando quiser realizar transações.

[028]Essa propriedade de descentralização pode ajudar a evitar o surgimento de um centro de gerenciamento em uma posição controlada. Por exemplo, a manutenção da blockchain de bitcoins é realizada pela rede de nós de comunicação do software de bitcoin na área de execução. Esta divulgação usa uma ou mais cadeias de blocos ou moedas digitais, como bitcoin e Ethereum, como exemplos. Uma pessoa com habilidade ordinária na técnica deve apreciar que as soluções técnicas divulgadas nesta divulgação podem usar ou se aplicar a outro tipo de cadeias de blocos e moedas digitais. Ou seja, em vez de bancos, instituições ou administradores no sentido tradicional, existem vários intermediários em uma forma de servidores que executam o software de bitcoin. Esses servidores de computador formam uma rede conectada via Internet, na qual qualquer pessoa pode se conectar potencialmente à rede. As transações acomodadas pela rede podem ser de uma forma: “o usuário A quer enviar Z bitcoins para o usuário B”, em que as transações são transmitidas para a rede usando aplicativos de software prontamente disponíveis. Os servidores do computador funcionam como servidores de bitcoin que operam para validar essas transações financeiras, adicionam um registro deles à sua cópia do ledger e, em seguida, transmitem essas adições de ledger para outros servidores da rede.

[029]Manter a blockchain é chamado de “mineração”, e aqueles que fazem essa manutenção são recompensados com bitcoins recém-criados e taxas de transação conforme mencionado anteriormente. Por exemplo, os nós podem determinar se as transações são válidas com base em um conjunto de regras com as quais a rede de blockchain concordou. Os mineradores podem estar localizados em qualquer continente e processar pagamentos verificando cada transação como válida e adicionando-a à blockchain. Tal verificação é alcançada através de consenso forne-

cido por uma pluralidade de mineradores e assume que não há colusão sistemática. No final, todos os dados serão consistentes, porque o cálculo deve atender a certos requisitos para ser válido e todos os nós serão sincronizados para garantir que a blockchain seja consistente. Assim, os dados podem ser consistentemente armazenados em um sistema distribuído de nós de blockchain.

[030]Através do processo de mineração, as transações como transferências de ativos são verificadas e adicionadas a uma cadeia crescente de blocos de uma blockchain por nós da rede. Ao atravessar toda a blockchain, a verificação pode incluir, por exemplo, se a parte pagadora tem acesso ao ativo transferido, se o ativo foi gasto antes, se o valor da transferência está correto, etc. Por exemplo, em uma transação hipotética (por exemplo, uma transação de bitcoins sob um modelo de UTXO (saída de transação não usada), uma transação de moedas de Ethereum sob um modelo de conta/ saldo) assinado por um emissor, a transação proposta pode ser transmitida para a rede de blockchain para a mineração. Um minerador precisa verificar se a transação está qualificada para ser executada de acordo com o histórico da blockchain. Se o balanço de carteira do emissor tiver fundos suficientes de acordo com a história blockchain existente, a transação é considerada válida e pode ser adicionada ao bloco. Uma vez verificada, as transferências de ativos podem ser incluídas no próximo bloco a ser adicionado à blockchain.

[031]Um bloco é muito parecido com um registro de banco de dados. Cada vez que grava-se dados cria-se um bloco. Esses blocos são ligados e protegidos usando criptografia para se tornarem redes interconectadas. Cada bloco é conectado ao bloco anterior, que é também 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 dados reais (por exemplo, dados de transação). A blockchain está ligada por meio dos cabe-

çalhos de bloco. Cada cabeçalho de bloco pode conter múltiplos valores de recursos, como versão, hash de bloco anterior, raiz de merkle, registro de dados, alvo de dificuldade e nonce. O hash de bloco anterior contém não apenas o endereço do bloco anterior, mas também o hash dos dados dentro do bloco anterior, tornando assim os cadeias de blocos imutáveis. O nonce é um número que, quando incluído, produz um hash com um número especificado de zero bits iniciais.

[032]Para mineração, o hash dos conteúdos do novo bloco é obtido por um nó. O nonce (por exemplo, string aleatória) é anexado ao hash para obter uma nova string. A nova string é novamente dividida. O hash final é então comparado ao alvo de dificuldade (por exemplo, um nível) e determinado se o hash final for realmente menor que o alvo de dificuldade ou não. Caso contrário, o nonce é alterado e o processo é repetido novamente. Se sim, então o bloco é adicionado à cadeia e o ledger público é atualizado e alertado sobre a adição. O nó responsável pela adição bem-sucedida é recompensado com bitcoins, por exemplo, adicionando uma transação de recompensa ao si próprio no novo bloco (conhecido como geração de moedas).

[033]Ou seja, para cada saída “Y”, se k é escolhido de uma distribuição com alta min-entropia, é inviável encontrar uma entrada x tal que H(k|x) = Y, onde K é o nonce, x é o hash de bloco, Y é o alvo de dificuldade e “|” indica concatenação. Por causa de hashes criptográficos serem essencialmente aleatórios, no sentido de que sua saída não pode ser prevista a partir de suas entradas, existe apenas uma maneira conhecida de encontrar o nonce: tentar inteiros um após o outro, por exemplo 1, depois 2, então 3 e assim por diante, o que pode ser conhecido como força bruta. Quanto maior o número de zeros à esquerda, mais se demorará, em média, a encontrar um requisito Y básico. 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 as capacidades de processamento do hardware de computação aumentam com o tempo, com o passar

dos anos, o protocolo de bitcoin exigirá mais bits zeros iniciais para que a mineração leve uma duração de cerca de dez minutos para ser implementada.

[034]Como descrito, o hashing é um marco importante para a blockchain. O algoritmo de hash pode ser entendido como uma função que comprime mensagens de qualquer tamanho em um resumo de mensagem de tamanho fixo. Mais comumente usados são MD5 e SHA. Em algumas modalidades, o comprimento de hash da blockchain é de 256 bits, o que significa que, independentemente do conteúdo original, um número binário de 256 bits é finalmente calculado. E pode ser garantido que o hash correspondente é único, desde que o conteúdo original seja diferente. Por exemplo, o hash da string "123" é a8fdc205a9f19cc1c7507a60c4f01b13d11d7fd0 (hexadecimal), que tem 256 bits quando convertido em binário, e apenas "123" tem esse hash. O algoritmo de hash na blockchain é irreversível, isto é, o cálculo direto é fácil (de "123" para a8fdc205a9f19cc1c7507a60c4f01b1c7507a60c4f01b13d11d7fd0), e o cálculo inverso não pode ser feito mesmo se todos os recursos de computação estiverem esgotados. Assim, o hash de cada bloco da blockchain é único.

[035]Além disso, se o conteúdo do bloco for alterado, seu hash será alterado. O bloco e o hash estão na correspondência de um para um, e o hash de cada bloco é calculado especificamente para o cabeçalho de bloco. Ou seja, os valores de recurso dos cabeçalhos de bloco são conectados para formar uma cadeia longa e, em seguida, o hash é calculado para a cadeia. Por exemplo, "Hash = SHA256 (cabeçalho de bloco)" é uma fórmula de cálculo de hash de bloco, SHA256 é um algoritmo de hash de blockchain aplicado ao cabeçalho de bloco. O hash é determinado exclusivamente pelo cabeçalho de bloco e não pelo corpo de bloco. Como mencionado acima, o cabeçalho de bloco contém muito conteúdo, incluindo o hash de bloco atual e o hash de bloco anterior. Isso significa que, se o conteúdo do bloco atual for alterado, ou se o hash de bloco anterior for alterado, ele causará uma alteração de

hash no bloco atual. Se o hacker modificar um bloco, o hash desse bloco se altera. Para que um bloco posterior se conecte ao bloco modificado, o hacker deve modificar todos os blocos subsequentes, pois o próximo bloco deve conter o hash de bloco anterior. Caso contrário, o bloco modificado será desconectado da blockchain. Devido a razões de projeto, os cálculos de hash são demorados, e é quase impossível modificar vários blocos em um curto período de tempo, a menos que o hacker domine mais de 51% da potência de computação de toda a rede. Assim, a blockchain garante sua própria confiabilidade e, uma vez que os dados são gravados, eles não podem ser adulterados.

[036]Uma vez que o minerador encontrar o hash (isto é, uma assinatura ou solução elegível) para o novo bloco, o minerador transmite esta assinatura para todos os outros mineradores (nós da blockchain). Outros mineradores agora verificam, por sua vez, se esta solução corresponde com o problema do bloco de emissor (isto é, determina se a entrada de hash efetivamente resulta na assinatura). Se a solução é válida, os outros mineradores vão confirmar a solução e concordarão que o novo bloco pode ser adicionado à blockchain. Assim, o consenso do novo bloco é alcançado. Isso também é conhecido como “prova de trabalho”. O bloco para o qual o consenso foi alcançado agora pode ser adicionado à blockchain e é transmitido para todos os nós na rede junto com sua assinatura. Os nós aceitarão o bloco e o salvarão em seus dados de transação, desde que as transações dentro do bloco correspondam corretamente aos saldos de carteira atuais (histórico de transações) naquele momento. Cada vez que um novo bloco é adicionado ao topo do bloco, a adição também conta como outra “confirmação” para os blocos antes disso. Por exemplo, se uma transação for incluída no bloco 502, e a blockchain tiver 507 blocos de comprimento, isso significa que a transação tem cinco confirmações (correspondente aos blocos 507 a 502). Quanto mais confirmações a transação tiver, mais difícil será para invasores alterarem.

[037]Em algumas modalidades, um sistema de ativos de blockchain exemplificador utiliza criptografia de chave pública, na qual são geradas duas chaves criptográficas, uma chave pública e uma chave privada. A chave pública pode ser considerada como um número de conta, e a chave privada pode ser considerada como credenciais de propriedade. Por exemplo, uma carteira de bitcoin é uma coleção de chaves públicas e privadas. A propriedade de um ativo (por exemplo, a moeda digital, ativo de dinheiro, estoques, ações, obrigações) associada a um determinado endereço de ativos pode ser demonstrada com o conhecimento da chave privada pertencente ao endereço. Por exemplo, o software de carteira de bitcoin, às vezes chamado de "software de cliente de bitcoin", permite que um determinado usuário transacione bitcoins. Um programa de carteira gera e armazena chaves privadas e se comunica com os pares na rede de bitcoin.

[038]Nas transações de blockchain, os pagadores e beneficiários são identificados na blockchain por suas chaves criptográficas públicas. Por exemplo, a maioria das transferências de bitcoin contemporâneas são de uma chave pública para uma chave pública diferente. Na prática os hashes destas chaves são usados na blockchain e são chamados "endereços de bitcoin". Em princípio, se uma pessoa invasora hipotética S pudesse roubar dinheiro da pessoa A simplesmente adicionando transações ao ledger de blockchain como "pessoa A paga à pessoa S 100 bitcoins", usando os endereços de bitcoin dos usuários em vez de seus nomes. O protocolo de bitcoin impede este tipo de roubo, exigindo que cada transferência seja assinada digitalmente com a chave privada do pagador, e só as transferências assinadas podem ser adicionadas para o ledger de blockchain. Como a pessoa S não pode forjar a assinatura da pessoa A, a pessoa S não pode fraudar a pessoa A adicionando uma entrada para o equivalente da blockchain para a "pessoa A paga à pessoa S 200 bitcoins." Ao mesmo tempo, qualquer pessoa pode verificar a assinatura da pessoa A usando sua chave pública e, portanto, que a mesma autorizou

qualquer transação na blockchain onde está o pagador.

[039]No contexto de transação de bitcoin, para transferir alguns bitcoins para o usuário B, o usuário A pode construir um registro contendo informações sobre a transação através de um nó. O registro pode ser assinado com a chave de assinatura do usuário A (chave privada) e conter a chave de verificação pública do usuário A e a chave de verificação pública do usuário B. A assinatura é usada para confirmar que a transação veio do usuário e também impede que a transação seja alterada por qualquer pessoa, uma vez que tenha sido emitida. O registro junto com outro registro que ocorreu na mesma janela de tempo em um novo bloco pode ser transmitido para os nós completos. Ao receber os registros, os nós completos podem trabalhar em incorporar os registros na borda de todas as transações que já ocorreram no sistema blockchain, adicionar o novo bloco a uma blockchain previamente aceita através do processo de mineração descrito acima, e validar o bloco adicionado de acordo com as regras de consenso da rede.

[040]O modelo de UTXO (saída de transação não usada) e um modelo de conta/saldo são dois modelos exemplificadores para a implementação da blockchain transações. Com UTXO, os ativos são representados por saídas de transações de cadeias de blocos 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 em uma forma de UTXO. Para gastar (transacionar) o ativo, o usuário A precisa assinar com a chave privada. O bitcoin é um exemplo de uma moeda digital que usa o modelo de UTXO. No caso de uma transação de rede de blocos válida, as saídas não usadas podem ser usadas para efetuar outras transações. Em algumas modalidades, apenas as saídas não usadas podem ser usadas em transações adicionais para evitar gastos duplos e fraude. Por esse motivo, as entradas em uma rede de blocos são excluídas quando ocorre uma transação e, ao mesmo tempo, as saídas são criadas na forma de UTXOs. Essas saídas de transação não usadas podem ser

usadas (pelos detentores das chaves privadas, por exemplo, pessoas com carteiras de moeda digital) para fins de transações futuras.

[041]Por outro lado, o modelo de conta/saldo (ou chamado de Modelo de Transação com base em Conta) mantém o controle do saldo de cada conta como um estado global. O saldo de uma conta é verificado para garantir que seja maior ou igual ao valor de transação de gasto. Um exemplo de como o Modelo de Conta/Equilíbrio funciona no Ethereum é fornecido:

[042]1. Alice ganha 5 ethers através da mineração. Está registrado no sistema que Alice tem 5 ethers.

[043]2. Alice quer dar ao Bob 1 ether, então o sistema irá primeiro deduzir 1 ether da conta de Alice, então Alice agora tem 4 ethers.

[044]3. O sistema então aumenta a conta de Bob em 1 ether. O sistema sabe que Bob tem 2 ethers para começar, portanto o saldo de Bob é aumentado para 3 ethers.

[045]A manutenção de registros para Ethereum pode ser assim como em um banco. Uma analogia é usar um cartão ATM/débito. O banco controla quanto dinheiro cada cartão de débito tem, e quando Bob precisa gastar o dinheiro, o banco verifica o seu registro para garantir que Bob tem saldo suficiente antes de aprovar a transação.

[046]Como a blockchain e outros ledgers similares são completamente públicos, a blockchain em si não tem proteção de privacidade. A natureza pública da rede P2P significa que, enquanto aqueles que a usam não são identificados pelo nome, as transações de vinculação a indivíduos e empresas é viável. Por exemplo, em remessas para o estrangeiro ou na cadeia de abastecimento, o valor de transação tem um nível extremamente elevado de valor de proteção de privacidade, porque com as informações de valor de transação, é possível inferir a localização específica e as identidades das partes da transação. O assunto da transação pode incluir,

por exemplo, dinheiro, token, moeda digital, contrato, escritura, registro médico, detalhe de clientes, estoques, obrigações, ações ou qualquer outro ativo que possa ser descrito na forma digital. Embora o modelo de UTXO possa fornecer anonimato aos valores de transação, por exemplo, através da assinatura de anel em Monero e na criptografia de conhecimento zero Zcash, os valores de transação permanecem desprotegidos no Modelo de Conta/Equilíbrio. Assim, um problema técnico abordado pela presente divulgação é como proteger a informação online, como a privacidade dos valores de transação. Tais transações podem estar no modelo de conta/saldo.

[047]Algumas tecnologias existentes propõem o uso do esquema de compromisso de Pedersen para criptografar o valor de transação e substituir o Modelo de Conta/Equilíbrio. De acordo com o esquema, o emissor envia o valor de transação e um número aleatório correspondente ao compromisso de Pedersen do valor de transação para o beneficiário através de um canal seguro fora da blockchain. O beneficiário verifica se o número aleatório corresponde ao compromisso da transação e executa o armazenamento local. Por exemplo, mediante o Modelo de Conta/Balanço, uma conta pode ser tratada como uma carteira (conta) para manter ativos que são agregados, mas não se mesclaram. Cada ativo pode corresponder a um tipo ativo (por exemplo, criptomoeda), e o saldo da conta é a soma dos valores de ativos. Mesmo os ativos do mesmo tipo não são mesclados. Durante a transação, um receptor de um ativo de transferência pode ser especificado, e o ativo correspondente pode ser removido da carteira para financiar a transação. Os nós de blockchain verificam se a carteira de pagamento possui ativo(s) suficiente(s) para cobrir a transação, e então os nós excluem o ativo transferido da carteira de pagamento e adicionam um ativo correspondente a uma carteira de receptor.

[048]No entanto, ainda existem limitações para esse esquema. O valor de transação e o número aleatório gerado pelo compromisso de Pedersen são dados sensíveis à privacidade. Partes que não aquelas relacionadas à transação não de-

vem ter a oportunidade de conhecer os valores. Assim, essas informações devem ser criptografadas e salvas e descriptografadas quando usadas. O valor comprometido e o número aleatório são elementos necessários para gastar o ativo transacionado em um tempo futuro, mas são fáceis de perder e difícil de recuperar por falta de seguro, estável, e forma eficiente para armazenar adequadamente números aleatórios. Por exemplo, o esquema das tecnologias atuais exige que o usuário mantenha um armazenamento persistente localmente para gerenciar os números aleatórios e os saldos de texto simples correspondentes ao saldo da conta criptografada, e a implementação do gerenciamento é complicada. Além disso, o armazenamento dos fatores de ocultação (por exemplo, os números aleatórios) e os saldos de texto simples que correspondem ao "ativo de Pedersen" em um único nó local é propenso à perda ou corrupção, enquanto o armazenamento de backup de múltiplos nós é difícil de realizar devido à alteração frequente do saldo da conta.

[049]Os sistemas e o método apresentados na presente divulgação podem ultrapassar as limitações acima e conseguir uma proteção de privacidade robusta para valores de transação, valores ativos, e fatores de ocultação em regimes de compromisso. Para esse fim, vários protocolos de troca de informações criptográficas podem ser usados para criptografar/descriptografar os números aleatórios e os saldos de texto simples, fornecendo assim gestão conveniente. Além disso, armazenar as informações criptografadas na blockchain garante que os valores de transação, os valores de ativos e os fatores de ocultação nos esquemas de compromisso não sejam facilmente perdidos ou adulterados.

[050]Em algumas modalidades, um esquema de compromisso (por exemplo, compromisso de Pedersen) pode criptografar determinado valor a (por exemplo, valor de transação, valor de ativo, parâmetro chave) da seguinte maneira:

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

[051]em que r é um fator de ocultação aleatório (alternativamente chamado

de fator de ligação) que fornece esconderijo, G e H são os geradores/pontos de base acordados publicamente da curva elíptica e podem ser escolhidos aleatoriamente, sn é o valor de 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 para os nós. Uma geração de "nada na minha manga" de H pode ser gerada fazendo o hash do ponto de base G com um mapeamento de função hash de um ponto para outro com H= Hash(G). H e G são os parâmetros públicos do dado sistema (por exemplo, os pontos gerados aleatoriamente em uma curva elíptica). Embora o acima forneça um exemplo de compromisso de Pedersen na forma de curva elíptica, várias outras formas de compromisso de Pedersen ou outros esquemas de compromisso podem ser alternativamente usadas.

[052]Um esquema de compromisso mantém o sigilo de dados, mas se compromete com os dados para que não possam ser alterados posteriormente pelo emissor de dados. Se uma parte só conhece o valor de compromisso (por exemplo, PC (a)), eles não podem determinar com que valores de dados subjacentes (por exemplo, a) se comprometeram. Ambos os dados (por exemplo, a) e o fator de ocultação (por exemplo, r) podem ser revelados posteriormente (por exemplo, pelo nó iniciador), e um receptor (por exemplo, nó de consenso) do compromisso pode executar o compromisso e verificar se os dados comprometidos correspondem aos dados revelados. O fator de ocultação está presente porque, sem um, alguém poderia tentar adivinhar os dados.

[053]Os esquemas de compromisso são uma forma de o emissor (parte de compromisso) se comprometer com um valor (por exemplo, a) tal que o valor comprometido permaneça privado, mas possa ser revelado em um momento posterior quando o consumador divulgar um parâmetro necessário do processo de compromisso. Esquemas de compromisso fortes podem ser tanto a ocultação de informações quanto a vinculação computacional. A ocultação refere-se à noção de que um

determinado valor a de um compromisso desse valor PC(a) deve ser não confiável. Ou seja, PC(a) não deve revelar nenhuma informação 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 vinculativo se não houver uma maneira plausível de que dois valores diferentes possam resultar no mesmo compromisso. Um compromisso de Pedersen é perfeitamente escondido e computacionalmente ligado sob a suposição de logaritmo discreto. Além disso, com r, G, H e PC(a) conhecidos, é possível verificar PC(a) determinando se PC(a) = r×G + a×H.

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

[055]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 pela multiplicação de um gerador pelo o grupo (G) com a chave secreta (Pub=rG. O resultado pode ser serializado como uma matriz de 33 bytes. As chaves públicas de ECC podem obedecer à propriedade homomórfica aditiva mencionada anteriormente em relação aos compromissos de Pedersen. Ou seja: Pub1+Pub2=(r1+r2(mod n))G.

[056]O compromisso de Pedersen para o valor de entrada pode ser criado escolhendo um gerador adicional para o grupo (H, nas equações abaixo) de forma que ninguém conheça o log discreto do segundo gerador H em relação ao primeiro

gerador G (ou vice-versa), ou seja, ninguém conhece um x tal que xG=H. Isso pode ser feito, por exemplo, usando o hash criptográfico de G para selecionar H: H = para_ _point(SHA256(ENCODE(G))).

[057]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 de ocultação secreto, e a pode ser o valor de entrada sendo comprometido. Portanto, se sn for comprometido, o esquema de compromisso PC(a) = r×G + a×H descrito acima pode ser obtido. Os compromissos de Pedersen são informações teoricamente privadas: para qualquer compromisso, existe algum fator de ocultação que faria qualquer quantia corresponder ao compromisso. Os compromissos de Pedersen podem ser computacionalmente seguros contra o falso compromisso, na medida em que o mapeamento arbitrário pode não ser computado.

[058]A parte (nó) que comprometeu o valor pode abrir o compromisso divulgando o valor original a e o fator r que completa a equação de compromisso. A parte que deseja abrir o valor PC(a) calculará o compromisso novamente para verificar se o valor original compartilhado realmente corresponde ao compromisso PC(a) inicialmente recebido. Assim, as informações do tipo de ativo podem ser protegidas mapeando-as para um número de série exclusivo e, em seguida, criptografando-as pelo compromisso de Pedersen. O número aleatório r escolhido ao gerar o compromisso torna quase impossível para qualquer um inferir o tipo de tipo de ativo que é comprometido de acordo com o valor de compromisso PC (a).

[059]Em algumas modalidades, vários protocolos de troca de informações criptográficos podem ser usados, como o protocolo de chave pública, protocolo de criptografia simétrica, troca de chave de Diffie-Hellman (DH), etc. Por exemplo, a troca de chaves de DH pode ser usada como um método para trocar seguramente chaves criptográficas por um canal público. A troca de chaves de DH, também cha-

mada de troca de chave exponencial, é um método de criptografia digital que usa números elevados à potências específicas para produzir chaves de descriptação com base em componentes que nunca são transmitidos diretamente, tornando a tarefa de um possível quebrador de códigos matematicamente opressiva.

[060]Em um exemplo de implementação de troca de chave de Diffie-Hellman (DH), os dois usuários finais Alice e Bob, ao se comunicarem através de um canal que eles sabem ser privado, concordam mutuamente com números inteiros positivos p e q, tal que p é um número primo e q é um gerador de p. O gerador de q é um número que, quando elevado a potências de números inteiros positivos menores que p, nunca produz o mesmo resultado para quaisquer dois 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 de p.

[061]Uma vez que Alice e Bob chegaram ao acordo sobre p e q em particular, eles escolhem chaves pessoais de um número inteiro positivo a e b, ambos menos do que o módulo de número primo p e ambos podem ser gerados aleatoriamente. Nenhum dos usuários divulga sua chave pessoal a ninguém e, idealmente, eles memorizam esses números e não os anotam nem os armazenam em lugar algum. Em seguida, Alice e Bob calculam as chaves públicas a* e b* com base em suas chaves pessoais de acordo com as fórmulas

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

e

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

[062]Os dois usuários podem compartilhar suas chaves públicas a* e b* em um meio de comunicação considerado inseguro, como a Internet ou uma rede de área ampla corporativa (WAN). A partir dessas chaves públicas, um número k1 pode ser gerado por qualquer usuário com base em suas próprias chaves pessoais.

[063] Alice calcula k1 usando a fórmula: $k1 = (b^*)^a \bmod p$

[064]Bob calcula k1 usando a fórmula: $k1 = (a^*)^b \bmod p$

[065]O valor de k1 é o mesmo de acordo com as duas fórmulas acima. No entanto, as chaves pessoais a e b, que são fundamentais para o cálculo de k1, não foram transmitidas através de um meio público. Mesmo com p, q, a* e b*, ainda é muito difícil calcular a e b. Por ser um número grande e aparentemente aleatório, um hacker em potencial quase não tem chance de adivinhar corretamente o k1, mesmo com a ajuda de um poderoso computador para realizar milhões de testes. Os dois usuários podem, portanto, em teoria, se comunicar de forma privada em um meio público com um método de criptografia de sua escolha usando a chave de descriptografia k1.

[066]Em um outro exemplo de implementação de troca de chaves de Diffie-Hellman (DH), todos os cálculos acontecem em um grupo discreto de tamanho suficiente, onde o problema de Diffie-Hellman é considerado difícil, geralmente o módulo de grupo multiplicativo um primo grande (por exemplo, para DH clássico) ou um grupo de curva elíptica (por exemplo, para a curva Elíptica de Diffie-Hellman).

[067]Para as duas partes, cada parte escolhe uma chave privada a ou b. Cada parte calcula a chave pública correspondente aG ou bG. Cada parte envia a chave pública aG ou bG para a outra parte. Cada parte usa a chave pública recebida juntamente com a sua própria chave privada para calcular o novo segredo compartilhado a(bG) = b(aG),, que pode então ser usado com uma função de derivação chave para derivar um conjunto de chaves para um esquema de criptografia simétrica. Alternativamente, vários outros métodos de computação podem ser usados, por exemplo, gerando chaves públicas g^a e g^b e uma chave compartilhada g^{ab} ou g^{ba}.

[068]Durante as transações, a proteção de informações é importante para proteger a privacidade do usuário, e o valor de transação é um tipo de informação que não tem proteção. A FIG. 1 mostra um sistema exemplificador 100 para proteção de informações, de acordo com várias modalidades. Como 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), os nós completos com determinado nível de poder de voto podem ser referidos como nós de consenso, que assumem a responsabilidade da verificação da transação. Nesta divulgação, nós completos, nós de consenso, ou outros nós equivalentes podem verificar a transação.

[069]Também, como mostrado na FIG. 1, o usuário A e o usuário B podem usar dispositivos correspondentes, como laptops e telefones celulares, servindo como nós leves para realizar transações. Por exemplo, o usuário A pode querer transacionar com o usuário B transferindo algum ativo na conta do usuário A para a conta do usuário B. O usuário A e o usuário B 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 receptor A que inicia uma transação com o dispositivo do usuário B referido como o nó receptor B. O nó A pode acessar a blockchain através da comunicação com o nó 1 e o nó B pode acessar a blockchain através da comunicação com o nó 2. Por exemplo, o nó A e o nó B podem enviar transações para a blockchain através do nó 1 e do nó 2 para solicitar a adição das transações à blockchain. Fora da blockchain, o nó A e o nó B podem ter outros canais de comunicação (por exemplo, comunicação regular pela Internet sem passar pelos nós 1 e 2).

[070]Cada um dos nós na FIG. 1 pode compreender um processador e um meio de armazenamento legível por computador não transitório acoplado ao processador, o meio de armazenamento armazenando instruções que, quando executadas pelo processador, fazem com que o nó (por exemplo, o processador) execute várias etapas para proteção de informações descrita aqui. Cada nó pode ser instalado com um software (por exemplo, programa de transações) e/ou hardware (por exemplo, fios, conexões sem fio) para se comunicar com outros nós e/ou outros dispositivos.

Mais detalhes do hardware e software do nó são descritos mais tarde com referência à FIG. 5

[071]A FIG. 2 ilustra etapas exemplificadoras para transação e verificação entre um nó emissor A, um nó receptor B e um ou mais nós de verificação, de acordo com várias modalidades. As operações apresentadas abaixo pretendem ser ilustrativas. Dependendo da implementação, as etapas exemplificadoras podem incluir etapas adicionais, poucas etapas ou etapas alternativas executadas em várias ordens ou em paralelo.

[072]Em várias modalidades, as contas de partes de transação (usuário emissor A e usuário receptor B) são configuradas para o modelo de Conta/Saldo. O usuário A e o usuário B podem executar as seguintes etapas para realizar a transação através de um ou mais dispositivos, como seu laptop, telefone celular, etc. Os dispositivos podem ser instalados com um software e hardware apropriados para executar as várias etapas. Cada conta pode estar associada a uma chave privada criptográfica (chave secreta) - par de chaves públicas. A chave privada pode ser denotada como SK, e a chave pública pode ser denotada como PK. A chave privada pode ser usada para assinar informações transmitidas (por exemplo, informações de transação). A chave pública pode ser usada para verificar as informações assinadas e gerar o endereço da conta. Cada conta pode conter vários ativos, cada um denotado como: ((V=PC(r, v), E_K(r, v)), onde v representa o valor de face do ativo, V representa um compromisso de Pedersen do valor de face v, ré um fator de ocultação (por exemplo, um número aleatório), PC () é um algoritmo de compromisso de Pedersen, E() é um algoritmo de criptografia n (por exemplo, algoritmo de criptografia de chave criptográfica) e K é uma chave de criptografia que é exclusiva para cada conta. Por exemplo, cada ativo pode ser denotado como (V=PC(r, v), E_K(r||v)), onde || representam a concatenação. Embora a concatenação seja usada nas seguintes modalidades, outras representações alternativas que envolvem r e v podem ser usa-

das. A chave de criptografia K (por exemplo, KA, KB) pode ser gerada por vários métodos, como protocolo de chave privada, função de derivação de chave, etc. Cada ativo também pode incluir informações diferentes das listadas, como as informações de origem do ativo.

[073]Em um exemplo, antes do usuário A transacionar com sucesso um valor t para o usuário B em uma transação verificada por blockchain, as abordagens e ativos na conta de A e na conta de B são os seguintes:

[074]Para a conta de A (conta A):

Endereço: AddrA

Chave pública: PK_A

Chave privada: SK_A

Primeira chave: K_A

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

(A_1=PC(r_{a1}, a_1), E_{KA}(r_{a1}, a_1)),

(A_2=PC(r_{a2}, a_2), E_{KA}(r_{a2}, a_2)),,

...

(A_m=PC(r_{am}, a_m), E_{KA}(r_{am}, a_m))

[075]Para o B conta (conta B):

Endereço: AddrB

Chave pública: PK_B

Chave privada: SK_B

Segunda chave: KB

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

(B_1=PC(r_{b1}, b_1), E_{KB}(r_{b1}, b_1)),

(B_2=PC(r_{b2}, b_2), E_{KB}(r_{b2}, b_2)),,

(B_n=PC(r_{bn}, b_n), E_{KB}(r_{bn}, b_n))

[076]Em algumas modalidades, na etapa 201, o nó A pode iniciar uma transação com o nó B. Por exemplo, o usuário A e o usuário B podem negociar um valor de transação t da conta A do usuário A para a conta B do usuário B. A conta A e a conta B podem corresponder às "carteiras" aqui descritas. A conta A pode ter um ou mais ativos. O ativo pode incluir, por exemplo, dinheiro, token, moeda digital, contrato, escritura, registro médico, detalhe de clientes, estoques, obrigações, ações ou qualquer outro ativo que possa ser descrito na forma digital. A conta B pode ter um ou mais ativos ou nenhum ativo. Cada ativo pode estar associado a várias informações de blockchain armazenadas em blocos da blockchain, as informações de blockchain compreendendo, por exemplo, NoteType representando o tipo de ativo, NoteID representando identificação exclusiva de ativo, valores de compromisso representando um valor de compromisso (por exemplo, compromisso de Pedersen) do valor de ativo, criptografia de número aleatório e valor de ativo, etc.

[077]Como descrito em relação à conta A, em algumas modalidades, os ativos A_1 a A_m, respectivamente, correspondem aos valores de ativo a_1 a a_m e os números aleatórios r_{a1} a r_{am}. Com base nos números aleatórios r_{a1} a r_{am}, o nó A pode comprometer os valores de ativos na conta A a um esquema de compromisso (por exemplo, o compromisso de Pedersen) para obter valores de compromisso criptografados. Por exemplo, para a conta A, os valores de compromisso criptografados podem ser PC_1 a PC_m, onde $PC_i = PC(r_{ai}, a_i) = r_{ai} \times G + a_i \times H$, G e H são conhecidos, e i é uma variável entre 1 e m. Além do primeiro PC de campo (...), cada ativo também está associado a um segundo campo E(...), conforme descrito anteriormente. O segundo campo E(...) pode representar uma criptografia do número aleatório correspondente e do valor de ativo criptografado com a chave KA. Por exemplo, a criptografia pode ser $E_{KA}(r_{ai}, a_i)$. O PC(...) e E(...) para cada ativo podem ser herdados de transações anteriores. O mesmo mecanismo pode se aplicar para a conta B e seus ativos.

[078]Em algumas modalidades, para satisfazer a quantidade de transação t, o usuário A pode usar uma primeira chave KA (por exemplo, uma chave de criptografia simétrica) para descriptografar um ou mais ativos de um valor agregado de, pelo menos, t da conta A. Por exemplo, o nó A pode explorar os ativos A_1, A_2, ..., A_k para esta transação, onde k é menor ou igual a m. Os ativos restantes A_{k+1}, A_{k+2}, ..., A_m da conta A são inexplorados. Correspondentemente, o nó A pode ler os ativos $PC(r_{a1}, a_1)$, $PC(r_{a2}, a_2)$, ..., $PC(r_{ak}, a_k)$ do nó 1. Com o número aleatório r_{a1}, r_{a2}, ..., r_{ak} conhecidos para o nó A, o nó A pode descriptografar a ativos de leitura $PC(r_{a1}, a_1)$, $PC(r_{a2}, a_2)$, ..., $PC(r_{ak}, a_k)$ para obter os valores dos ativos a_1, a_2, ..., a_k para garantir que a soma $(a_1 + a_2 + ... + a_k)$ não seja inferior ao valor de transação t. Ativos diferentes podem ser trocados entre si dentro da conta com base em várias taxas.

[079]Em algumas modalidades, a chave de criptografia simétrica pode se referi às mesmas chaves criptográficas usadas no algoritmo de chave simétrica criptográfica para criptografia de texto simples e decriptação de texto codificado. As chaves podem ser idênticas ou elas podem ter uma transformação simples entre as duas chaves. As chaves podem representar um segredo compartilhado entre duas ou mais partes que podem ser usados para manter um link de informações privadas.

[080]Em algumas modalidades, a quantidade de valor ativo selecionado em excesso de t, se houver, é definida como y como a alteração. Por exemplo, o nó A pode determinar a alteração $y = (a_1 + a_2 + ... + a_k) - t$. Um nó A pode selecionar números aleatórios r_t e r_y como fatores de ocultação 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 para um esquema de compromisso (por exemplo, criptografia homomórfica) para obter o valor de compromisso $T = PC(r_t, t)$, e comprometer y e r_y em um esquema de compromisso (por exemplo, criptografia homomórfica) para obter o valor de compromisso $Y = PC(r_y, y)$. Além disso, o nó A pode determinar $r' = (r_1 + r_2 ... + r_k) - r_t$ -

r_y.

[081]Em algumas modalidades, o nó A pode usar a primeira chave KA para criptografar (r_y, y), obtendo a criptografia $E_{KA}(r_y, y)$. O nó A pode armazenar $E_{KA}(r_y, y)$ localmente.

[082]Na etapa 202, nó A pode enviar a informação de transação para nó B (por exemplo, através de blockchain, através de um canal seguro fora do bloco de cadeia). A informação de transação enviada pode compreender, por exemplo, o número aleatório r_t, o valor de transação t, e valor de compromisso T. As informações da transação podem ser enviadas em texto simples.

[083]Na etapa 203, o nó B pode verificar o número aleatório r_t, o valor de transação t e o valor de compromisso T. Em algumas modalidades, o nó B pode verificar se o valor t para enviar ao usuário B está correto e se $T=PC(r_t, t)$. Para a etapa 203, se a correspondência/verificação falhar, o nó B pode rejeitar a transação. Se a correspondência/verificação for bem sucedida, o nó B pode responder ao nó A na etapa 204.

[084]Na etapa 204, o nó B pode criptografar (r_t, t) com uma segunda chave KB (por exemplo, um chave de criptografia simétrica) para obter a criptografia $E_{KB}(r_t, t)$ e assinar a transação ($E_{KB}(r_t, t)$, T) com a chave privada do usuário B, SK_B, para gerar uma assinatura SIGB. A assinatura pode seguir o Algoritmo de Assinatura Digital (Digital Signature Algorithm, DSA) tal como o Algoritmo de Assinatura Digital Curva Elíptica (Elliptic Curve Digital Signature Algorithm, ECDSA), onde o receptor da assinatura pode verificar a assinatura com a chave pública de assinaturas para autenticar os dados assinados. A assinatura SIGB indica que o nó receptor B concorda com a transação.

[085]Na etapa 205, o nó B pode transmitir a transação assinada $E_{KB}(r_t, t)$ e a assinatura SIGB de volta ao nó A.

[086]Na etapa 206, se SIGB não é for verificada com sucesso, o nó A pode

rejeitar a transação. Se o SIGB for verificada com sucesso, o nó A pode gerar uma prova RP para provar os nós de blockchain se o valor de PC(r_t, t) e o valor de PC(r_y, y) estiverem dentro de um intervalo válido; por exemplo, para ter valores validados de PC(r_t, t), o valor de transação t pode estar dentro de um intervalo válido [0, 2^n-1]; e ter valores válidos de PC(r_y, y), a alteração y pode estar dentro de um intervalo válido [0, 2^n-1]. Em uma modalidade, o nó A pode usar a técnica de prova de bloco para gerar a prova RP de alcance relacionada com (T, r_t, t, Y, r_y, y) para os nós das cadeias de blocos (por exemplo, os nós de consenso) verificarem em uma etapa posterior se o valor de transação t e a alteração y estão dentro do intervalo válido com base na prova de alcance. A prova de alcance pode incluir, por exemplo, Bulletproofs, assinatura de anel Borromean, etc.

[087]Além disso, o nó A pode assinar a transação com a chave privada SK_A do usuário A para gerar uma assinatura SIGA. Da mesma forma, a assinatura pode seguir o Algoritmo de Assinatura Digital (DSA). Em uma modalidade, o nó A pode assinar ({PC(r_{a1}, a_1), E_{KA}(r_{a1}, a_1); PC(r_{a2}, a_2), E_{KA}(r_{a2}, a_2); ... PC(r_{ak}, a_k), E_{KA}(r_{ak}, a_k)}; {PC(r_y, y), E_{KA}(r_y, y)}; {PC(r_t, t), E_{KB}(r_t, t)}; Y; T; r'; RP) com a chave privada do usuário A para gerar a assinatura SIGA, onde {PC(r_{a1}, a_1), E_{KA}(r_{a1}, a_1); PC(r_{a2}, a_2), E_{KA}(r_{a2}, a_2); ... PC(r_{ak}, a_k), E_{KA}(r_{ak}, a_k)} representa os ativos explorados A_1, A_2, ..., A_k da conta A para a transação. {PC(r_y, y), E_{KA}(r_y, y)} representa a alteração que a conta A receberá da transação. {PC(r_t, t), E_{KB}(r_t, t)} representa o ativo transferido que a conta B receberá da transação.

[088]Na etapa 207, o nó A pode submeter a transação para a blockchain, fazendo com que os nós da blockchain verifiquem a transação e determinem se a transação deve ser adicionada à blockchain. Em uma modalidade, o nó A pode submeter a transação ({PC(r_{a1}, a_1), E_{KA}(r_{a1}, a_1); PC(r_{a2}, a_2), E_{KA}(r_{a2}, a_2); ... PC(r_{ak}, a_k), E_{KA}(r_{ak}, a_k)}; {PC(r_y, y), E_{KA}(r_y, y)}; {PC(r_t, t), E_{KB}(r_t, t)}; Y; T; r'; RP; SIGA; SIGB) para a blockchain através do nó 1 para executar a transação. A transação pode in-

cluir parâmetros adicionais ou pode não incluir todos os parâmetros listados. A transação pode ser transmitida para um ou mais nós (por exemplo, nós de consenso) na blockchain para verificação. Se a verificação for bem-sucedida, a transação será adicionada à blockchain. Se a verificação falhar, a transação será rejeitada da adição à blockchain.

[089]Nas etapas 208 a 213, os um ou mais nós (por exemplo, nós de consenso) verificam as assinaturas, a prova de alcance, e outra informação 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 conta separadamente.

[090]Em algumas modalidades, para executar a transação, as informações de transação podem ser verificadas por vários nós de blockchain. As informações de transação podem incluir o endereço de transação TXID, assinatura (s), entrada e saída. TXID pode compreender o hash do conteúdo da transação. As assinaturas podem incluir assinaturas de chave criptografada pelo emissor e receptor. A entrada pode incluir um endereço da conta do emissor na blockchain, um ou mais ativos explorados da conta de blockchain do emissor para transação, etc. A saída pode compreender um endereço da conta do receptor em blockchain, tipo(s) de ativo do(s) ativo(s) do receptor, valor(es) de compromisso do(s) ativo(s) de receptor, etc. A entrada e a saída podem compreender informações indexadas em um formulário tabular. Em algumas modalidades, o valor do valor de NoteID pode ser “o TXID + um índice do ativo na saída”.

[091]Em algumas modalidades, o um ou mais nós da blockchain pode verificar a transação submetida ({$PC(r_{a1}, a_1)$, $E_{KA}(r_{a1}, a_1)$; $PC(r_{a2}, a_2)$, $E_{KA}(r_{a2}, a_2)$; ... $PC(r_{ak}, a_k)$, $E_{KA}(r_{ak}, a_k)$}; {$PC(r_y, y)$, $E_{KA}(r_y, y)$}; {$PC(r_t, t)$, $E_{KB}(r_t, t)$}; Y; T; r'; RP; SIGA; SIGB).

[092]Na etapa 208, os nós podem verificar se a transação foi executada

usando um mecanismo anti-gasto duplo ou um mecanismo de ataque anti-repetição. Se a transação foi executada, os nós podem rejeitar a transação; caso contrário, o método pode prosseguir para a etapa 209.

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

[094]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 ativo no tipo de Nota para A_1 a A_k são consistentes com o(s) tipo(s) de ativo(s) do valor de transação t. Se algum dos tipos de ativos for inconsistente, os nós podem rejeitar a transação; caso contrário, o método pode prosseguir para a etapa 211. Em algumas modalidades, o tipo de ativo original na carteira pode ter sido convertido para outro tipo com base em uma taxa de câmbio, e esta etapa pode ser ignorada.

[095]Na etapa 211, os nós podem verificar a prova de alcance 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 RP de alcance para verificar se o valor de transação t não é menor do que zero e a alteração y não é menor do que zero. Se a verificação falhar, os nós podem rejeitar a transação; caso contrário, o método pode prosseguir para a etapa 212.

[096]Na etapa 212, os nós podem verificar se as entradas e as saídas da transação são consistentes. Em uma modalidade, r' pode corresponder ao valor de ativo $t' = a_1 + a_2 \ldots + a_k - t - y$ com base na propriedade homomórfica, em que $r' = (r_1 + r_2 \ldots + r_k) - r_t - r_y$. Uma vez que os ativos de entrada são $a_1 + a_2 \ldots + a_k$ e a saída é $t + y$, $t' = 0$ quando a entrada e saída são consistentes: $a_1 + a_2 \ldots + a_k = t + y$. Assim, o valor de compromisso correspondente a r' é $PC(r', t') = r' \times G + t' \times H = r'G$. Um vez que $r' = (r_1 + r_2 \ldots + r_k) - r_t - r_y$, os nós podem determinar se as entradas e saídas são

iguais, verificando se r'G é igual a $PC_1 + \ldots + PC_k - T - Y$ correspondente a $(r_1 + r_2 \ldots + r_k) - r_t - r_y$. Se r'G for igual a $PC_1 + \ldots + PC_k - T - Y$, os nós podem determinar que as entradas e as saídas da transação são consistentes e prosseguir para a próxima etapa; caso contrário, os nós podem determinar que as entradas e saídas da transação são inconsistentes e rejeitam a transação.

[097]Na etapa 213, os nós podem verificar se o nó A possui o(s) ativo(s) explorado(s) para a transação. Em uma modalidade, os nós podem executar esta verificação com base na informação armazenada na blockchain, tal como informação correspondente à conta A. A informação pode compreender informação de transação anterior de todos os ativos. Os nós podem, portanto, determinar se a conta A possui o ativo de transação para a transação. Se a determinação for não, os nós podem rejeitar a transação; caso contrário, o método pode prosseguir para a etapa 214.

[098]Na etapa 214, os nós podem atualizar a conta A e a conta B. Por exemplo, os nós podem remover o ativo de transação do valor t da conta A e adicionar o mesmo à conta B. Com base na propriedade homomórfica, como $Y = PC(r_y, y)$ e o nó 1 conhece r_y e pode acessar o valor de compromisso Y da blockchain, o nó 1 pode descriptografar Y para obter o valor de ativo 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 da blockchain o valor de compromisso T. Assim, o nó 2 pode descriptografar T para obter o valor de ativo t e adicionar o mesmo à conta B.

[099]Em um exemplo, Após a actualização de conta A e da conta B, a conta A recebe a alteração y para os ativos explorado $A_1, A_2, \ldots, A_k$ e recebe a seus ativos não explorados $A_{ak+1}, \ldots, A_m$, e a conta B recebe o valor de transação t e recebe seus ativos originais $B_1, B_2, \ldots, B_n$. Os ativos na conta A e na conta de B são os seguintes:

[0100]Para a conta de A (conta A), os ativos atualizados são denotados co-

mo:

$(Y=PC(r_y, y), E_{KA}(r_y, y))$,

$(A_{ak+1}=PC(r_{ak+1}, a_{k+1}), E_{KA}(r_{ak+1}, a_{k+1}))$

$(A_{ak+2}=PC(r_{ak+2}, a_{k+2}), E_{KA}(r_{ak+2}, a_{k+2}))$

...

$(A_m=PC(r_{am}, a_m), E_{KA}(r_{am}, a_m))$

[0101]Para a conta de B (conta B), os ativos atualizados são denotados como:

$(B_1=PC(r_{b1}, b_1), E_{KB}(r_{b1}, b_1))$,

$(B_2=PC(r_{b2}, b_2), E_{KB}(r_{b2}, b_2))$,

...

$(B_n=PC(r_{bn}, b_n), E_{KB}(r_{bn}, b_n))$,

$(T=PC(r_t, t), E_{KB}(r_t, t))$

[0102]Embora essa divulgação use o nó A/usuário A e o nó B/usuário B para ilustrar o emissor e o receptor, respectivamente, o emissor e o receptor podem ser o mesmo nó/usuário. Por exemplo, a alteração y de uma transação (total de ativos explorados na conta A menos o valor de transação) pode ser enviada de volta ao emissor da transação. Assim, as várias etapas realizadas pelo nó B, como aqui descrito, podem ser alternativamente realizadas pelo nó A.

[0103]A FIG. 3 ilustra um fluxograma de um método exemplificador 300 para proteção de informações, de acordo com várias modalidades da presente divulgação. O método 300 pode ser implementado por um ou mais componentes (por exemplo, nó A, nó 1, uma combinação de nó A e nó 1) do sistema 100 da FIG. 1. O método 300 pode ser implementado por um sistema ou dispositivo (por exemplo, computador, servidor) compreendendo um processador e um meio de armazenamento legível por computador não transitório (por exemplo, memória) armazenando instruções. As instruções, quando executadas pelo processador, fazem com que o

sistema ou dispositivo (por exemplo, o processador) realize o método 300. As operações do método 300 apresentadas abaixo têm a intenção de ser ilustrativas. Dependendo da implementação, o método exemplificador 300 pode incluir etapas adicionais, poucas etapas ou etapas alternativas executadas em várias ordens ou em paralelo.

[0104]O bloco 301 compreende: comprometer um valor de transação t de uma transação com um primeiro esquema de compromisso para obter um valor de compromisso de transação T, e comprometer uma alteração y da transação com um segundo esquema de compromisso para obter um valor de compromisso de alteração Y, o primeiro esquema de compromisso compreendendo um fator de ocultação de transação r_t, e o segundo esquema de compromisso compreendendo um fator de ocultação de alteração r_y. Em algumas modalidades, o primeiro esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator de ocultação de transação r_t e com o valor de transação t sendo um valor de compromisso correspondente. Veja, por exemplo, $T=PC(r_t, t)$. O segundo esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator de ocultação de alteração r_y e com a alteração y sendo um valor de compromisso correspondente. Veja, por exemplo, $Y=PC(r_y, y)$.

[0105]O Bloco 302 compreende: criptografar uma primeira combinação do fator de ocultação de alteração r_y e a alteração y com uma primeira chave KA.

[0106]O Bloco 303 compreende: transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de compromisso de transação T para um nó receptor associado a um receptor de transação para o nó receptor verificar a transação. Em algumas modalidades, transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de compromisso de transação T para o nó receptor associado ao receptor de transação para o nó receptor verificar a transação compreende: transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de

compromisso de transação T com o nó receptor associado ao receptor de transação, fazendo com que o nó receptor verifique se o valor de compromisso de transação T é igual ao primeiro esquema de compromisso comprometendo o valor de transação t com o fator de ocultação de transação r_t.

[0107]O bloco 304 compreende: em resposta ao fato de que o nó receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocultação de transação r_t e do valor de transação t criptografado com uma segunda chave KB. Em algumas modalidades, a obtenção da segunda combinação criptografada compreende receber do nó receptor a segunda combinação criptografada e uma assinatura SIGB associada com a segunda combinação criptografada e o valor de compromisso de transação T.

[0108]O Bloco 305 compreende: transmitir a primeira combinação criptografada e a segunda combinação criptografada a uma pluralidade de nós em uma blockchain para os nós na blockchain verificarem a transação.

[0109]Em algumas modalidades, o valor de transação t é explorado de um ou mais ativos A_1, A_2, ..., A_k de um emissor da transação; cada um dos ativos está associado a (1) um compromisso de Pedersen com base pelo menos em um fator de ocultação r_{ak} e um valor de cada ativo e (2) uma criptografia com base pelo menos no fator de ocultação r_{ak} e o valor de cada ativo; e a alteração y é uma diferença entre o valor de transação t e os ativos explorados.

[0110]Em algumas modalidades, antes de transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós na blockchain, o método compreende ainda: verificar a assinatura SIGB; e em resposta à verificação bem-sucedida da assinatura SIGB, gerar uma assinatura SIGA associada aos ativos A_1, A_2, ..., A_k, a primeira combinação, a segunda combinação, o valor de compromisso de transação T, o valor de compromisso de alteração Y e uma diferença entre uma soma de fatores de ocultação correspondentes aos ativos A_1, A_2,

..., A_k e uma soma do fator de ocultação de transação r_t e o fator de ocultação de alteração r_y. Ou seja, a diferença $r' = (r_1 + r_2 \ldots + r_k) - (r_t + r_y)$.

[0111]Em algumas modalidades, a transmissão da primeira combinação criptografada e da segunda combinação criptografada para a pluralidade de nós na blockchain compreende: transmitir os ativos A_1, A_2, ..., A_k, a primeira combinação, a segunda combinação, a valor de compromisso de transação T, o valor de compromisso de alteração Y, uma diferença entre uma soma de fatores de ocultação correspondentes aos ativos A_1, A_2, ..., A_k e uma soma do fator de ocultação de transação r_t e do fator de ocultação da alteração r_y, a assinatura SIGA e a assinatura SIGB para a pluralidade de nós na blockchain.

[0112]Em algumas modalidades, a transmissão da primeira combinação criptografada e da segunda combinação criptografada para a pluralidade de nós em uma blockchain para os nós na blockchain para verificar a transação compreende: transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós em uma blockchain, fazendo com que os nós na blockchain, em resposta à verificação bem-sucedida da transação, emitam o valor de transação t para o receptor, eliminem os ativos A_1, A_2, ..., A_k, e emitam a alteração y para o emissor.

[0113]A FIG. 4 ilustra um fluxograma de um método exemplificador 400 para proteção de informações, de acordo com várias modalidades da presente divulgação. O método 400 pode ser implementado por um ou mais componentes (por exemplo, nó B, nó 2, uma combinação do nó B e do nó 2, etc.) do sistema 100 da FIG. 1. O método 400 pode ser implementado por um sistema ou dispositivo (por exemplo, computador, servidor) compreendendo um processador e um meio de armazenamento legível por computador não transitório, (por exemplo, memória), que armazena as instruções. As instruções, quando executadas pelo processador, fazem com que o sistema ou dispositivo (por exemplo, o processador) execute o método

400. As operações do método 400 apresentadas abaixo pretendem ser ilustrativas. Dependendo da implementação, o método exemplificador 400 pode incluir etapas adicionais, menos etapas ou etapas alternativas executadas em várias ordens ou em paralelo.

[0114]O Bloco 401 compreende: obter um fator de ocultação de transação r_t, um valor de transação t de uma transação e um valor de compromisso de transação T de um nó emissor associado a um emissor de uma transação, em que: o valor de transação t é comprometido com um primeiro esquema de compromisso para obter o valor de compromisso de transação T, o primeiro esquema de compromisso compreendendo o fator de ocultação de transação r_t.

[0115]O Bloco 402 compreende: verificar a transação com base no fator de ocultação de transação r_t obtido, no valor de transação t obtido de uma transação, e no valor de compromisso de transação T obtido. Em algumas modalidades, verificar a transação com base no fator de ocultação de transação r_t obtido, no valor de transação t obtido de uma transação e no valor de compromisso de transação obtido T compreende verificar se o valor de compromisso de transação obtido T é igual ao primeiro esquema de compromisso que compromete o valor de transação t obtido com o fator de ocultação de transação r_t obtido.

[0116]O Bloco 403 compreende: em resposta à verificação bem-sucedida da transação, criptografar uma segunda combinação do fator de ocultação de transação r_t e o valor de transação t com uma segunda chave KB.

[0117]O Bloco 404 compreende: transmitir a segunda combinação criptografada para o nó emissor. Em algumas modalidades, antes de transmitir a segunda combinação criptografada ao nó emissor, compreendendo ainda gerar uma assinatura SIGB associada com a segunda combinação criptografada e o valor de compromisso de transação T; e transmitir a segunda combinação criptografada para o nó emissor compreende transmitir a segunda combinação criptografada e a assinatura

SIGB ao nó emissor.

[0118]Como mostrado, a privacidade para o valor de transação pode ser protegida através de várias melhorias da tecnologia de computação. Por exemplo, a estrutura da conta compreende um ou mais campos, como um primeiro campo associado ao compromisso de Pedersen do valor de ativo (por exemplo, o primeiro campo sendo $PC(r_{ai}, ai)$, com i sendo entre 1 e m) e um segundo campo associado ao número aleatório para o compromisso de Pedersen e o valor de ativo (por exemplo, o segundo campo sendo $E_{KA}(r_{ai}, ai)$, com i sendo entre 1 e m). O primeiro campo e o segundo campo também são usados nas etapas da transação e armazenados na blockchain.

[0119]Para outro exemplo, uma chave criptográfica é usada para criptografar o número aleatório de cada compromisso de Pedersen e o valor de ativo correspondente. A chave criptográfica para criptografia/descriptografia é mantida pelo proprietário da conta, portanto, a privacidade dos valores do ativo é protegida dos usuários sem a chave criptográfica. Além disso, a transação, incluindo os números aleatórios criptografados e os valores dos ativos, é armazenada na blockchain. Essa maneira fornece conveniência para gerenciar os números aleatórios, minimiza as chances de perda e alteração dos números aleatórios e valores de ativos e promove a segurança com base no armazenamento de blockchain distribuído e consistente.

[0120]As etapas antes de submeter a transação à blockchain podem ser tratadas como comportamento “fora da cadeia” ou “pré-transação”, pois os processos de criptografia e descriptografia acontecem no lado do cliente, enquanto a blockchain armazena o “valor do ativo + número aleatório correspondente” criptografado representado pela função E(). O compromisso de Pedersen pode ser semelhante a um cofre com ativos internos, e o “valor de ativo + número aleatório correspondente” é semelhante à chave do cofre. A chave criptografada e seu cofre associado podem ser armazenados na blockchain, que é à prova de temperatura e antiperda. Toda

vez que o usuário deseja gastar o(s) ativo(s), o usuário pode recuperar o cofre e a chave criptografada da blockchain e descriptografar a chave no lado do cliente, para que as etapas de "pré-transação" possam ser executadas para montar uma nova transação que gasta o(s) ativo(s).

[0121]Como tal, os números aleatórios de compromissos de Pedersen podem ser convenientemente gerenciados, sem o risco de corrupção e sem incorrer em encargos de gerenciamento de chaves adicionais. Assim, a privacidade da transação pode ser totalmente protegida, e os valores das transações podem ser mantidos em segredo.

[0122]As técnicas descritas aqui são implementadas por um ou mais dispositivos de computação para fins especiais. Os dispositivos de computação para fins especiais podem ser sistemas de computadores desktop, sistemas de computadores servidores, sistemas de computadores portáteis, dispositivos portáteis, dispositivos de rede ou qualquer outro dispositivo ou combinação de dispositivos que incorporam a lógica hard-wired e/ou de programa para implementar as técnicas. O(s) dispositivo(s) de computação são geralmente controlados e coordenados pelo software do sistema operacional. Os sistemas operacionais convencionais controlam e agendam processos de computador para execução, executam gerenciamento de memória, fornecem sistema de arquivos, rede, serviços de I/O e fornecem uma funcionalidade de interface de usuário, como uma interface gráfica de usuário ("GUI"), entre outras coisas.

[0123]A FIG. 5 é um diagrama de blocos que ilustra um sistema de computador 500 sobre o qual qualquer uma das modalidades aqui descritas pode ser implementada. O sistema 500 pode ser implementado em qualquer um dos nós aqui descritos e configurado para realizar as etapas correspondentes para métodos de proteção de informações. O sistema de computador 500 inclui um barramento 502 ou outro mecanismo de comunicação para informação de comunicação, um ou mais

processador(es) de hardware(s) 504 acoplado(s) com o barramento 502 para o processamento de informações. O(s) processador(es) de hardware 504 podem ser, por exemplo, um ou mais microprocessadores de propósito geral.

[0124]O sistema de computador 500 também inclui uma memória principal 506, tal como uma memória de acesso aleatório (RAM), cache e/ou outros dispositivos de armazenamento dinâmicos, acoplados ao barramento 502 para armazenar informações e instruções a serem executadas pelo(s) processador(es) 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 pelo(s) processador(es) 504. Tais instruções, quando armazenadas em meios de armazenamento acessíveis ao(s) processador(es) 504, processa o sistema de computador 500 em uma máquina de propósito especial que é personalizada para executar as operações especificadas nas instruções. O sistema de computador 500 inclui ainda uma memória somente de leitura (ROM) 508 ou outro dispositivo de armazenamento estático acoplado ao barramento 502 para armazenar informação estática e instruções para processador(es) 504. Um dispositivo de armazenamento 510, tal como um disco magnético, disco óptico, ou pen drive USB (Flash drive), etc., é fornecido e acoplado ao barramento 502 para armazenar informações e instruções.

[0125]O sistema de computador 500 pode implementar as técnicas descritas aqui usando lógica hardwired personalizada, um ou mais ASICs ou FPGAs, firmware e/ou lógica de programa que em combinação com o sistema de computador provoca ou programa o sistema de computador 500 para ser uma máquina com propósito especial. De acordo com uma modalidade, as operações, métodos e processos descritos são aqui executados pelo sistema de computador 500 em resposta ao(s) processador(es) 504 que executa(m) uma ou mais sequências de uma ou mais instruções contidas na memória principal 506. Tais instruções podem ser lidas na memória

principal 506 de outro meio de armazenamento, tal como o dispositivo de armazenamento 510. A execução das sequências de instruções contidas na memória principal 506 faz com que o(s) processador(es) 504 execute(m) as etapas do processo aqui descritas. Em modalidades alternativas, circuitos hardwired podem ser usados em vez de ou em combinação com instruções de software.

[0126]A memória principal 506, a ROM 508 e/ou o armazenamento 510 podem incluir meios de armazenamento não transitórios. O termo “meio não transitório” e termos similares, como usados aqui, se referem a meios que armazenam dados e/ou instruções que fazem com que uma máquina opere de maneira específica, o meio exclui sinais transitórios. Esses meios não transitórios podem incluir meios não voláteis e/ou meios voláteis. A mídia não volátil inclui, por exemplo, discos ópticos ou magnéticos, como o dispositivo de armazenamento 510. A mídia volátil inclui memória dinâmica, como a memória principal 506. Formas comuns de meio não transitório incluem, por exemplo, um disquete, uma disco flexível, disco rígido, unidade de estado sólido, fita magnética ou qualquer outro meio de armazenamento de dados magnético, um CD-ROM, qualquer outro meio de armazenamento óptico de dados, qualquer meio físico com padrões de furos, uma memória RAM, uma memória PROM e uma memória EPROM, uma memória FLASH-EPROM, NVRAM, qualquer outro chip ou cartucho de memória e versões em rede dos mesmos.

[0127]O sistema de computador 500 também inclui uma interface de rede 518 acoplada ao barramento 502. A interface de rede 518 fornece um acoplamento de comunicação de dados bidirecionais para um ou mais links de rede que estão conectados a uma ou mais redes locais. Por exemplo, a interface de rede 518 pode ser uma placa de rede digital de serviços integrados (ISDN), modem de cabo, modem de satélite ou um modem para fornecer um link de comunicação de dados para um tipo de linha telefônica correspondente. Como outro exemplo, a interface de rede 518 pode ser uma placa de rede local (LAN) para fornecer uma conexão de comuni-

cação de dados a uma LAN compatível (ou componente de WAN para se comunicar com uma WAN). Links sem fio também podem ser implementados. Em qualquer implementação deste tipo, a interface de rede 518 envia e recebe sinais elétricos, eletromagnéticos ou ópticos que transportam fluxos de dados digitais representando vários tipos de informação.

[0128]O sistema de computador 500 pode enviar mensagens e receber dados, incluindo código de programa, através da(s) rede(s), 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.

[0129]O código recebido pode ser executado pelo(s) processador(es) 504 à medida que é recebido e/ou armazenado no dispositivo de armazenamento 510, ou outro armazenamento não volátil para execução posterior.

[0130]Cada um dos processos, métodos e algoritmos descritos nas seções anteriores podem ser incorporados e totalmente ou parcialmente automatizados por módulos de código executados por um ou mais sistemas de computador ou processadores de computador compreendendo hardware de computador. Os processos e algoritmos podem ser implementados parcialmente ou totalmente em circuitos específicos de aplicativos.

[0131]Os vários recursos e processos descritos acima podem ser usados independentemente uns dos outros, ou podem ser combinados de várias maneiras. Todas as combinações e subcombinações possíveis devem estar dentro do escopo desta divulgação. Além disso, determinados métodos ou blocos de processos podem ser omitidos em algumas implementações. Os métodos e processos aqui descritos também não estão limitados a qualquer sequência particular, e os blocos ou estados a eles relacionados podem ser realizados em outras sequências que sejam apropriadas. Por exemplo, os blocos ou estados descritos podem ser realizados em

uma ordem diferente da especificamente divulgada, ou múltiplos blocos ou estados podem ser combinados em um único bloco ou estado. Os blocos ou estados 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 divulgadas. Os sistemas e componentes exemplificadores aqui descritos podem ser configurados de maneira diferente do descrito. Por exemplo, elementos podem ser adicionados, removidos ou rearranjados em comparação com as modalidades exemplificadoras divulgadas.

[0132]As várias operações dos métodos exemplificadores aqui descritos podem ser realizadas, pelo menos parcialmente, por um algoritmo. O algoritmo pode estar compreendido em códigos de programa ou instruções armazenadas em uma memória (por exemplo, um meio de armazenamento legível por computador não transitório descrito acima). Tal algoritmo pode compreender um algoritmo de aprendizado de máquina. Em algumas modalidades, algoritmo de aprendizado de máquina não pode programar explicitamente os computadores para executar uma função, mas pode aprender a partir de dados de treinamento para fazer um modelo de previsões que executa a função.

[0133]As várias operações de métodos exemplificadores aqui descritas podem ser realizadas, pelo menos parcialmente, por um ou mais processadores que são temporariamente configurados (por exemplo, por software) ou permanentemente configurados para executar as operações relevantes. Configurados temporária ou permanentemente, tais processadores podem constituir mecanismos implementados pelo processador que operam para executar uma ou mais operações ou funções descritas aqui.

[0134]De modo similar, os métodos descritos aqui podem ser pelo menos parcialmente implementados em processador, com um processador ou processadores em particular sendo um exemplo de hardware. Por exemplo, pelo menos algu-

mas das operações de um método podem ser realizadas por um ou mais processadores ou mecanismos implementados pelo processador. Além disso, um ou mais processadores também podem operar para suportar o desempenho das operações relevantes em um ambiente de "computação em nuvem" ou como um "software como serviço" (SaaS). Por exemplo, pelo menos algumas das operações podem ser realizadas por um grupo de computadores (como exemplos de máquinas, incluindo processadores), sendo essas operações acessíveis por uma rede (por exemplo, a Internet) e por uma ou mais interfaces apropriadas (por exemplo, uma Interface de Programação de Aplicação (API)).

[0135]O desempenho de algumas das operações pode ser distribuído entre os processadores, não residindo apenas em uma única máquina, mas implantado em várias máquinas. Em algumas modalidades exemplificadoras, os processadores ou mecanismos implementados pelo processador podem estar localizados em uma única localização geográfica (por exemplo, dentro de um ambiente doméstico, um ambiente de escritório ou um farm de servidores). Em outras modalidades exemplificadoras, os processadores ou motores implementados por processador podem ser distribuídos através de várias localizações geográficas.

[0136]Ao longo deste relatório descritivo, casos plurais podem implementar componentes, operações ou estruturas descritas como um único caso. Embora operações individuais de um ou mais métodos sejam ilustradas e descritas como operações separadas, uma ou mais das operações individuais podem ser executadas simultaneamente, e nada requer que as operações sejam executadas na ordem ilustrada. Estruturas e funcionalidades apresentadas como componentes separados em configurações exemplificadoras podem ser implementadas como uma estrutura ou componente combinado. Da mesma forma, as estruturas e funcionalidades apresentadas como um único componente podem ser implementadas como componentes separados. Estas e outras variações, modificações, adições e melhorias estão den-

tro do escopo do assunto aqui tratado.

[0137]Embora tenha sido descrita uma descrição geral do assunto com referência a modalidades exemplificadoras específicas, podem ser feitas várias modificações e alterações a estas modalidades sem se distanciar do escopo mais amplo de modalidades da presente divulgação. Tais modalidades da matéria podem ser aqui referidas, individual ou coletivamente, pelo termo “invenção” apenas por conveniência e sem intenção de limitar voluntariamente o escopo deste pedido de patente a qualquer divulgação ou conceito único se mais de uma for, de fato divulgada. A Descrição Detalhada não deve ser tomada em um sentido limitativo, e o escopo de várias modalidades é definido apenas pelas reivindicações anexas, juntamente com a faixa completa de equivalentes a que tais reivindicações têm direito.

REIVINDICAÇÕES

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

comprometer um valor de transação t de uma transação com um primeiro esquema de compromisso para obter um valor de compromisso de transação T e comprometer uma alteração y da transação com um segundo esquema de compromisso para obter um valor de compromisso de alteração de Y, o primeiro esquema de compromisso compreendendo um fator de ocultação de transação r_t, e o segundo esquema de compromisso compreendendo um fator de ocultação de alteração r_y;

criptografar uma primeira combinação do fator de ocultação de alteração r_y e a alteração y com uma primeira chave KA;

transmitir o fator de ocultação de transação r_t, o valor de transação t, e o valor de compromisso de transação T para um nó receptor associado a um receptor de transação para o nó receptor verificar a transação;

em resposta ao fato de que o nó receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocultação de transação r_t e o valor de transação t criptografado com uma segunda chave KB; e

transmitir a primeira combinação criptografada e a segunda combinação criptografada para uma pluralidade de nós em uma blockchain para os nós na blockchain para verificar a transação.

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

o primeiro esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator de ocultação de transação r_t e com o valor de transação t sendo um valor comprometido correspondente; e

o segundo esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator de ocultação de alteração r_y e com a alteração

y sendo um valor correspondente comprometido.

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que transmitir o fator de ocultação de transação $r_{t,}$ o valor de transação T, e o valor de compromisso de transação T para o nó receptor relacionado com o receptor de transação para o nó receptor verificar a transação compreende:

transmitir o fator de ocultação de transação $r_{t,}$ o valor de transação t, e o valor de compromisso de transação T para o nó receptor associado ao receptor de transação, fazendo com que o nó receptor verifique se o valor de compromisso de transação T é igual ao primeiro esquema de compromisso comprometendo o valor de transação t com o fator de ocultação de transação $r_{t.}$

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

obter a segunda combinação criptografada compreende receber a partir do nó receptor a segunda combinação criptografada e uma assinatura SIGB associada com a segunda combinação criptografada e o valor de compromisso de transação T.

5. Método, de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que:

o valor de transação t é explorado de um ou mais ativos A_1, A_2, ..., A_k de um emissor da transação;

cada um dos ativos está associado a (1) um compromisso de Pedersen com base pelo menos em um fator de ocultação r_{ak} e um valor de cada ativo e (2) uma criptografia com base pelo menos no fator de ocultação r_{ak} e no valor de cada ativo; e

a alteração y é uma diferença entre o valor de transação t e os ativos explorados.

6. Método, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que, antes de transmitir a primeira combinação criptografada e a segunda combina-

ção criptografada para a pluralidade de nós na blockchain, compreende ainda:

verificar a assinatura SIGB; e

em resposta à verificação bem-sucedida da assinatura SIGB, gerar uma assinatura SIGA associada aos ativos A_1, A_2,..., A_k, a primeira combinação, a segunda combinação, o valor de compromisso de transação T, o valor de compromisso de alteração Y e um diferença entre uma soma de fatores de ocultação correspondentes aos ativos A_1, A_2, ..., A_k e uma soma do fator de ocultação de transação r_t e o fator de ocultação de alteração r_y.

7. Método, de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós na blockchain compreende:

transmitir os ativos A_1, A_2, ..., A_k, a primeira combinação, a segunda combinação, o valor de compromisso de transação T, o valor de compromisso de alteração Y, uma diferença entre uma soma de fatores de ocultação correspondentes aos ativos A_1, A_2, ..., A_k e uma soma do fator de ocultação de transação r_t e o fator de ocultação de alteração r_y, a assinatura SIGA, e a assinatura SIGB para a pluralidade de nós na blockchain.

8. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós da blockchain para os nós na blockchain para verificar a transação compreende:

transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós na blockchain, fazer com que os nós na blockchain, em resposta à verificação bem-sucedida da transação, emitam o valor de transação t para o receptor, eliminem os ativos A_1, A_2, ..., A_k, e emitam a alteração y para o emissor.

9. Meio de armazenamento legível por computador não transitório que arma-

zena instruções que, quando executadas por um processador, fazem com que o processador realize operações **CARACTERIZADO** pelo fato de compreende:

comprometer um valor de transação t de uma transação com um primeiro esquema de compromisso para obter um valor de compromisso de transação T e comprometer uma alteração y da transação com um segundo esquema de compromisso para obter um valor de compromisso de alteração Y, o primeiro esquema de compromisso compreendendo um fator de ocultação de alteração r_t, e o segundo esquema de compromisso compreendendo um fator de ocultação de alteração r_y;

criptografar uma primeira combinação do fator de ocultação de alteração r_y e a alteração y com uma primeira chave KA;

transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de compromisso de transação T para um nó receptor associado a um receptor de transação para o nó receptor verificar a transação;

em resposta ao fato de que o nó receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocultação de transação r_t e do valor de transação t criptografado com uma segunda chave KB; e

transmitir a primeira combinação criptografada e a segunda combinação criptografada a uma pluralidade de nós em uma blockchain para os nós na blockchain para verificar a transação.

10. Meio de armazenamento, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que:

o primeiro esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator de ocultação de transação r_t e com o valor de transação t sendo um valor de compromisso correspondente; e

o segundo esquema de compromisso compreende um compromisso de Pedersen com base pelo menos no fator de ocultação de alteração r_y e com a alteração y sendo um valor de compromisso correspondente.

11. Meio de armazenamento, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que transmitir o fator de ocultação de transação r_t, o valor de transação T, e o valor de compromisso de transação T para o nó receptor relacionado com o receptor de transação para o nó receptor verificar a transação compreende:

transmitir o fator de ocultação de transação r_t, o valor de transação t e o valor de compromisso de transação T para o nó receptor associado ao receptor de transação, fazendo com que o nó receptor verifique se o valor de compromisso de transação T é igual ao primeiro esquema de compromisso comprometendo o valor de transação t com o fator de ocultação de transação r_t.

12. Meio de armazenamento, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que:

obter a segunda combinação criptografada compreende receber a partir do nó receptor a segunda combinação criptografada e uma assinatura SIGB associada com a segunda combinação criptografada e o valor de compromisso de transação T.

13. Meio de armazenamento, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que:

o valor de transação t é explorado de um ou mais ativos A_1, A_2, ..., A_k de um emissor da transação;

cada um dos ativos está associado a (1) um compromisso de Pedersen com base pelo menos em um fator de ocultação r_{ak} e um valor de cada ativo e (2) uma criptografia com base, pelo menos, no fator de ocultação r_{ak} e o valor de cada de ativos; e

a alteração y é uma diferença entre o valor de transação t e os ativos explorados.

14. Meio de armazenamento, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que, antes de transmitir a primeira combinação crip-

tografada e a segunda combinação criptografada para a pluralidade de nós na blockchain, as operações compreendem ainda:

verificar a assinatura SIGB; e

em resposta à verificação bem-sucedida da assinatura SIGB, gerar uma assinatura SIGA associada aos ativos A_1, A_2,..., A_k, a primeira combinação, a segunda combinação, o valor de compromisso de transação T, o valor de compromisso de alteração Y e um diferença entre uma soma de fatores de ocultação correspondentes aos ativos A_1, A_2, ..., A_k e uma soma do fator de ocultação de transação r_t e do fator de ocultação de alteração r_y.

15. Meio de armazenamento, de acordo com a reivindicação 14, **CARACTERIZADO** pelo fato de que transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós na blockchain compreende:

transmitir os ativos A_1, A_2,..., A_k, a primeira combinação, a segunda combinação, o valor de compromisso de transação T, o valor de compromisso de alteração Y, uma diferença entre uma soma de fatores de ocultação correspondentes aos ativos A_1, A_2,..., A_k e uma soma do fator de ocultação de transação r_t e do fator de ocultação de alteração r_y, a assinatura SIGA, e a assinatura SIGB para a pluralidade de nós na blockchain.

16. Meio de armazenamento, de acordo com a reivindicação 15, **CARACTERIZADO** pelo fato de que transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós na blockchain para os nós na blockchain para verificar a transação compreende:

transmitir a primeira combinação criptografada e a segunda combinação criptografada para a pluralidade de nós na blockchain, fazendo com que os nós na blockchain, em resposta à verificação bem-sucedida da transação, emitam o valor de transação t para o receptor, eliminem os ativos A_1, A_2,..., A_k e emitam a alteração

y para o emissor.

17. Sistema de proteção de informações, **CARACTERIZADO** pelo fato de que compreende um processador e um meio de armazenamento legível por computador não transitório acoplado ao processador, o meio de armazenamento armazenando instruções que, quando executadas pelo processador, fazem com que o sistema realize operações compreendendo:

comprometer um valor de transação t de uma transação com um primeiro esquema de compromisso para obter um valor de compromisso de transação T e comprometer uma alteração y da transação com um segundo esquema de compromisso para obter um valor de compromisso de alteração Y, o primeiro esquema de compromisso compreendendo um fator de ocultação de transação r_t, e o segundo esquema de compromisso compreendendo um fator de ocultação de alteração r_y;

criptografar uma primeira combinação do fator de ocultação de alteração r_y e a alteração y com uma primeira chave KA;

transmitir o fator de ocultação de transação r_t, o valor de transação t, e o valor de compromisso de transação T para um nó receptor associado a um receptor de transação para o nó receptor verificar a transação;

em resposta ao fato de que o nó receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocultação de transação r_t e do valor de transação t criptografado com uma segunda chave KB; e

transmitir a primeira combinação criptografada e a segunda combinação criptografada a uma pluralidade de nós em uma blockchain para os nós na blockchain para verificar a transação.

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

obter um fator de ocultação de transação r_t, um valor de transação t de uma transação, e um valor de compromisso de transação T de um nó emissor associado

a um emissor de uma transação, em que: o valor de transação t é comprometido com um primeiro esquema de compromisso para obter o valor de compromisso de transação T, o primeiro esquema de compromisso compreendendo o fator de ocultação de transação r_t;

verificar a transação com base no fator de ocultação de transação r_t obtido, no valor de transação t obtido de uma transação, e no valor de compromisso de transação T obtido;

em resposta à verificação bem-sucedida da transação, criptografar uma segunda combinação do fator de ocultação de transação r_t e do valor de transação t com uma segunda chave KB; e

transmitir a segunda combinação criptografada ao nó emissor.

19. Método, de acordo com a reivindicação 18, **CARACTERIZADO** pelo fato de que:

verificar a transação com base no fator de ocultação de transação r_t obtido, no valor de transação t obtido de uma transação, e no valor de compromisso de transação T obtido compreende a verificação de se o valor de compromisso de transação T obtido é igual ao primeiro esquema de compromisso comprometendo o valor de transação t obtido com o fator de ocultação de transação r_t obtido.

20. Método, de acordo com a reivindicação 18, **CARACTERIZADO** pelo fato de que:

antes de transmitir a segunda combinação criptografada ao nó emissor, compreendendo ainda gerar uma assinatura SIGB associada com a segunda combinação criptografada e o valor de compromisso de transação T; e

transmitir a segunda combinação criptografada para o nó emissor compreende transmitir a segunda combinação criptografada e a assinatura SIGB ao nó emissor.

21. Método, de acordo com a reivindicação 18, **CARACTERIZADO** pelo fato

de que:

o primeiro esquema de compromisso compreende um compromisso de Pedersen com base, pelo menos, no fator de ocultação de transação r_t e com o valor de transação t sendo um valor de compromisso correspondente.

22. Meio de armazenamento legível por computador não transitório, que armazena instruções que, quando executadas por um processador, fazem com que o processador realize operações **CARACTERIZADO** pelo fato de que compreende:

obter um fator de ocultação de transação r_t, um valor de transação t de uma transação, e um valor de compromisso de transação T de um nó emissor associado a um emissor de uma transação, em que: o valor de transação t é comprometido com um primeiro esquema de compromisso para obter o valor de compromisso de transação T, o primeiro esquema de compromisso compreendendo o fator de ocultação de transação r_t;

verificar a transação com base no fator de ocultação de transação r_t obtido, no valor de transação t obtido de uma transação e no valor de compromisso de transação obtido T;

em resposta à verificação com sucesso da transação, criptografar uma segunda combinação do fator de ocultação de transação r_t e do valor de transação t com uma segunda chave KB; e

transmitir a segunda combinação criptografada para o nó emissor.

23. Sistema para proteção de informações, **CARACTERIZADO** pelo fato de que compreende um processador e um meio de armazenamento legível por computador não transitório acoplado ao processador, o meio de armazenamento armazenando instruções que, quando executadas pelo processador, fazem com que o sistema realize operações compreendendo:

obter um fator de ocultação de transação r_t, um valor de transação t de uma transação e um valor de compromisso de transação T de um nó emissor associado a

um emissor de uma transação, em que: o valor de transação t é comprometido com um primeiro esquema de compromisso para obter o valor de compromisso de transação T, o primeiro esquema de compromisso compreendendo o fator de ocultação de transação r_t;

verificar a transação com base no fator de ocultação de transação r_t obtido, no valor de transação t obtido de uma transação e no valor de compromisso de transação T obtido;

em resposta à verificação com sucesso da transação, criptografar uma segunda combinação do fator de ocultação de transação r_t e do valor de transação t com uma segunda chave KB; e

transmitir a segunda combinação criptografada para o nó emissor.

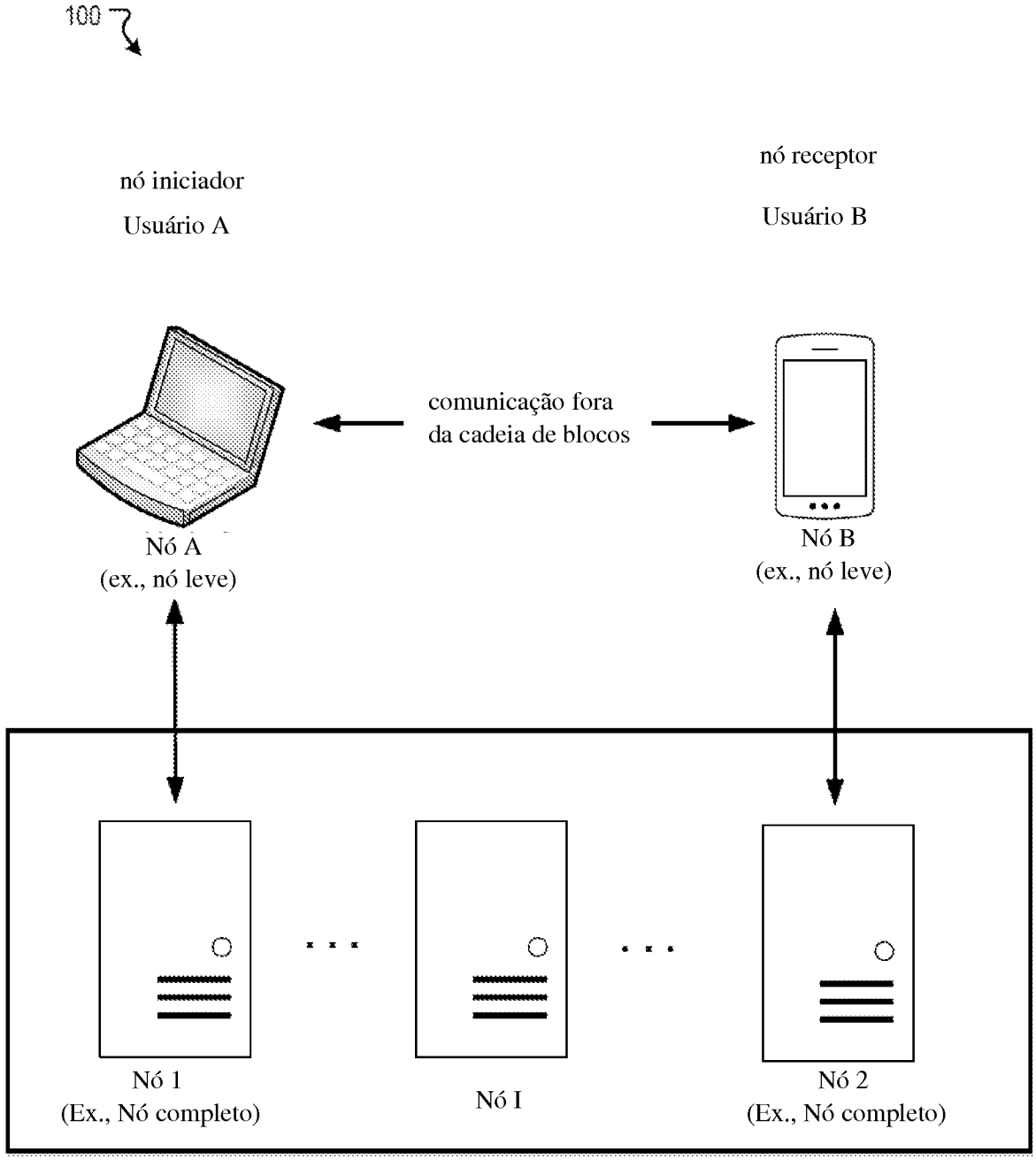

100
nó iniciador
Usuário A
nó receptor
Usuário B
comunicação fora
da cadeia de blocos
Nó A
(ex., nó leve)
Nó B
(ex., nó leve)
Nó 1
(Ex., Nó completo)
Nó I
Nó 2
(Ex., Nó completo)

FIG. 1

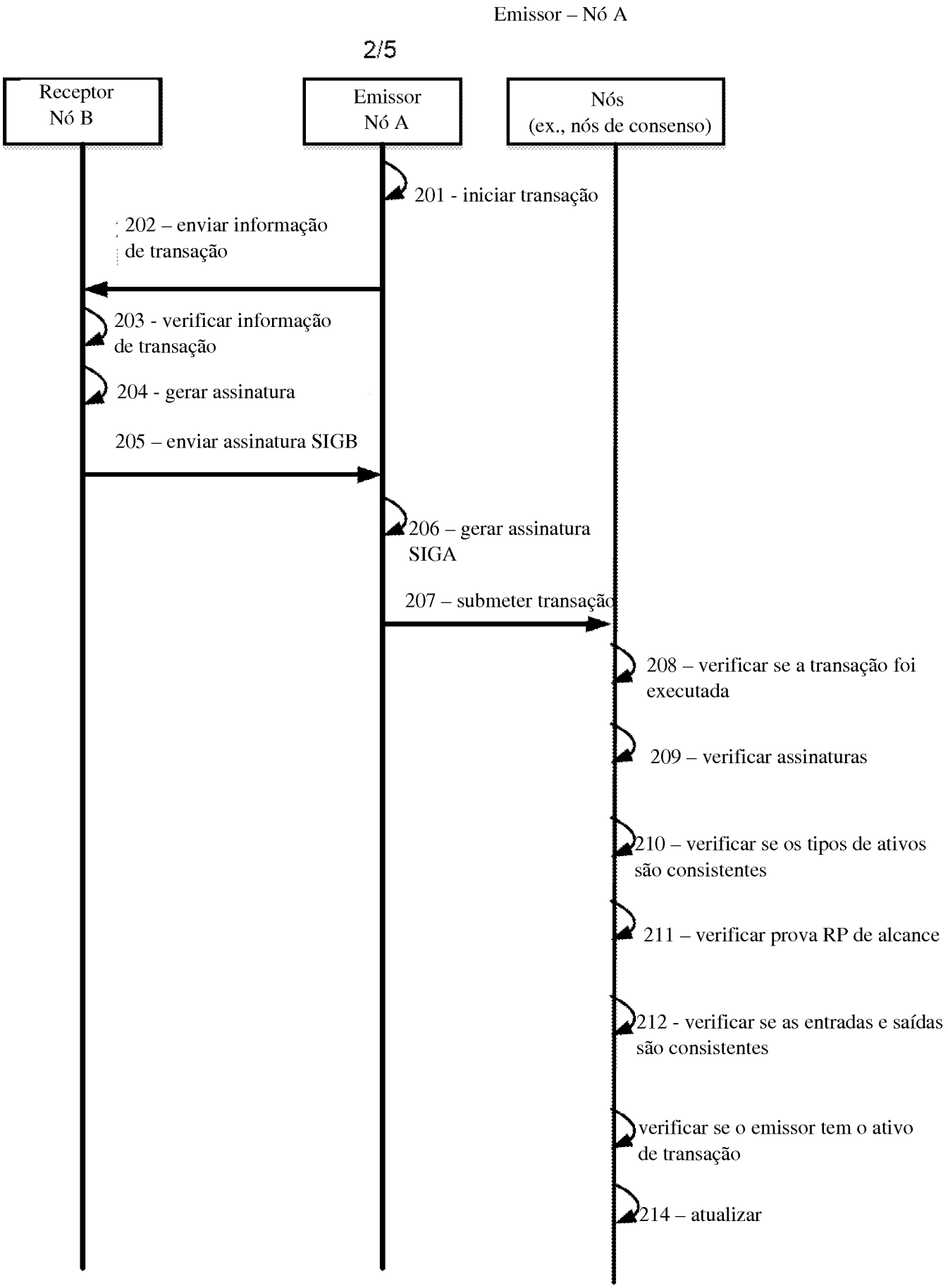

Emissor – Nó A
Receptor
Nó B
Emissor
Nó A
Nós
(ex., nós de consenso)
201 - iniciar transação
202 – enviar informação
de transação
203 - verificar informação
de transação
204 - gerar assinatura
205 – enviar assinatura SIGB
206 – gerar assinatura
SIGA
207 – submeter transação
208 – verificar se a transação foi
executada
209 – verificar assinaturas
210 – verificar se os tipos de ativos
são consistentes
211 – verificar prova RP de alcance
212 - verificar se as entradas e saídas
são consistentes
verificar se o emissor tem o ativo
de transação
214 – atualizar

FIG. 2

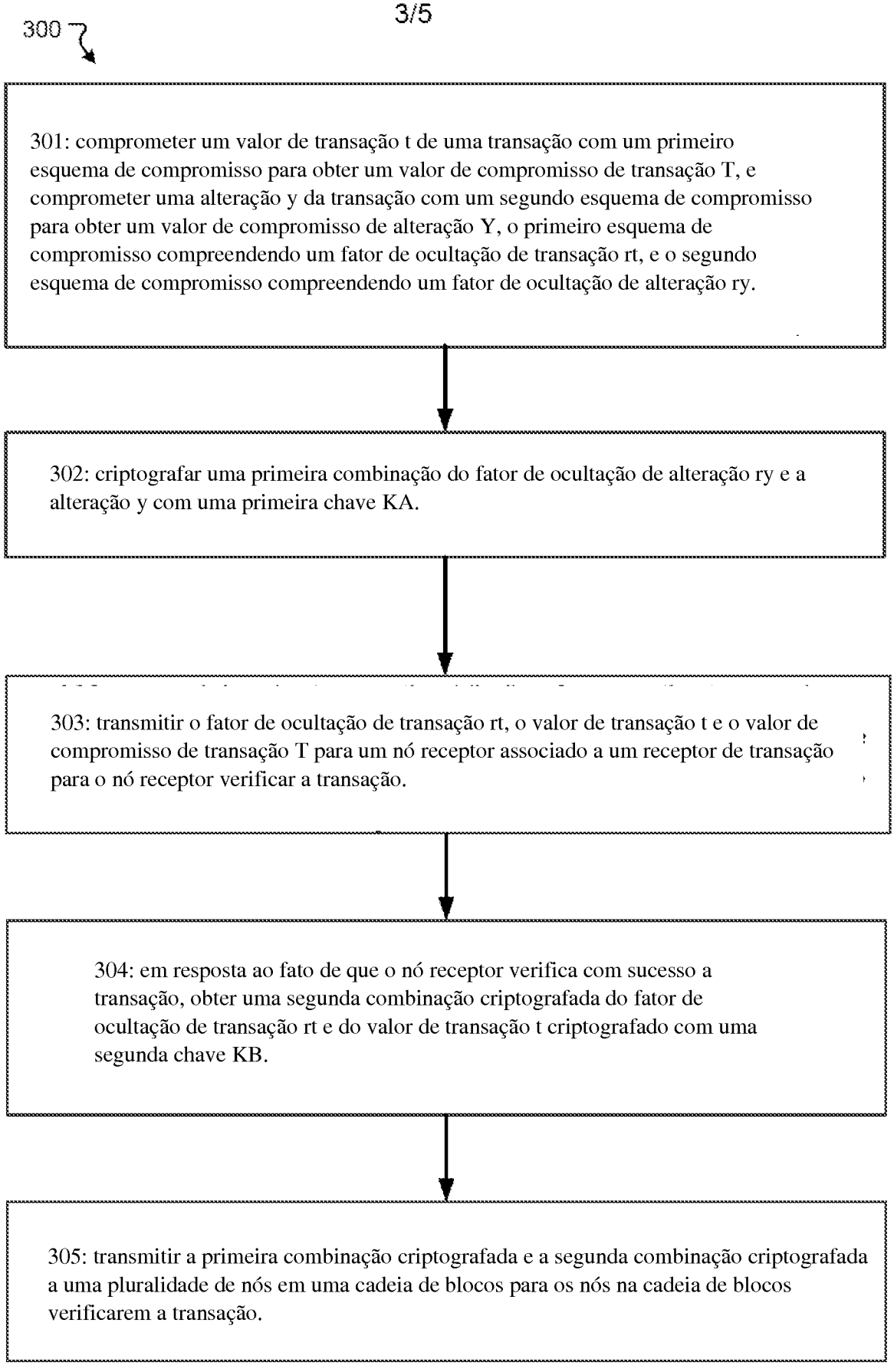

300
301: comprometer um valor de transação t de uma transação com um primeiro esquema de compromisso para obter um valor de compromisso de transação T, e comprometer uma alteração y da transação com um segundo esquema de compromisso para obter um valor de compromisso de alteração Y, o primeiro esquema de compromisso compreendendo um fator de ocultação de transação rt, e o segundo esquema de compromisso compreendendo um fator de ocultação de alteração ry.
302: criptografar uma primeira combinação do fator de ocultação de alteração ry e a alteração y com uma primeira chave KA.
303: transmitir o fator de ocultação de transação rt, o valor de transação t e o valor de compromisso de transação T para um nó receptor associado a um receptor de transação para o nó receptor verificar a transação.
304: em resposta ao fato de que o nó receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocultação de transação rt e do valor de transação t criptografado com uma segunda chave KB.
305: transmitir a primeira combinação criptografada e a segunda combinação criptografada a uma pluralidade de nós em uma cadeia de blocos para os nós na cadeia de blocos verificarem a transação.

FIG. 3

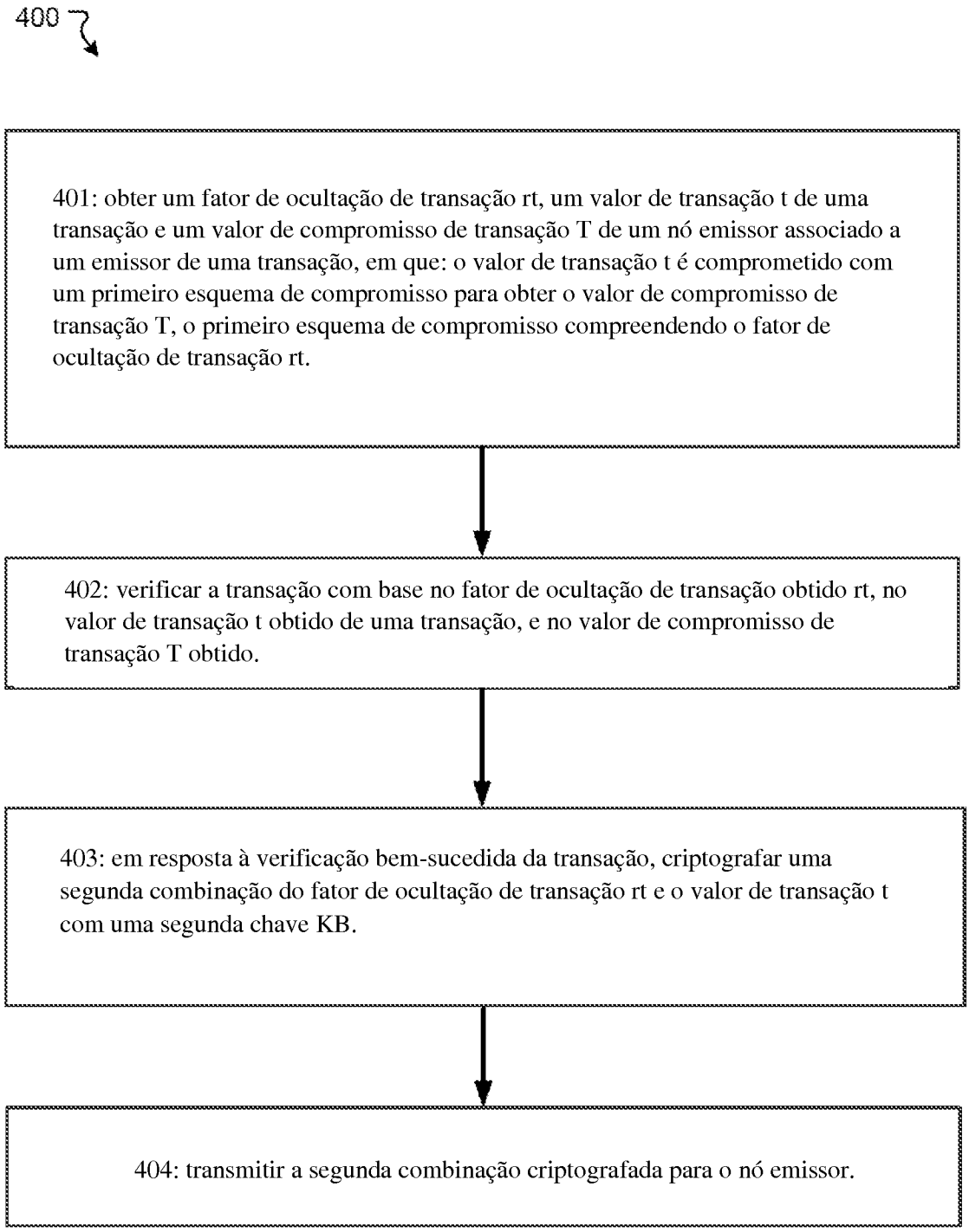

400
401: obter um fator de ocultação de transação rt, um valor de transação t de uma transação e um valor de compromisso de transação T de um nó emissor associado a um emissor de uma transação, em que: o valor de transação t é comprometido com um primeiro esquema de compromisso para obter o valor de compromisso de transação T, o primeiro esquema de compromisso compreendendo o fator de ocultação de transação rt.
402: verificar a transação com base no fator de ocultação de transação obtido rt, no valor de transação t obtido de uma transação, e no valor de compromisso de transação T obtido.
403: em resposta à verificação bem-sucedida da transação, criptografar uma segunda combinação do fator de ocultação de transação rt e o valor de transação t com uma segunda chave KB.
404: transmitir a segunda combinação criptografada para o nó emissor.

FIG. 4

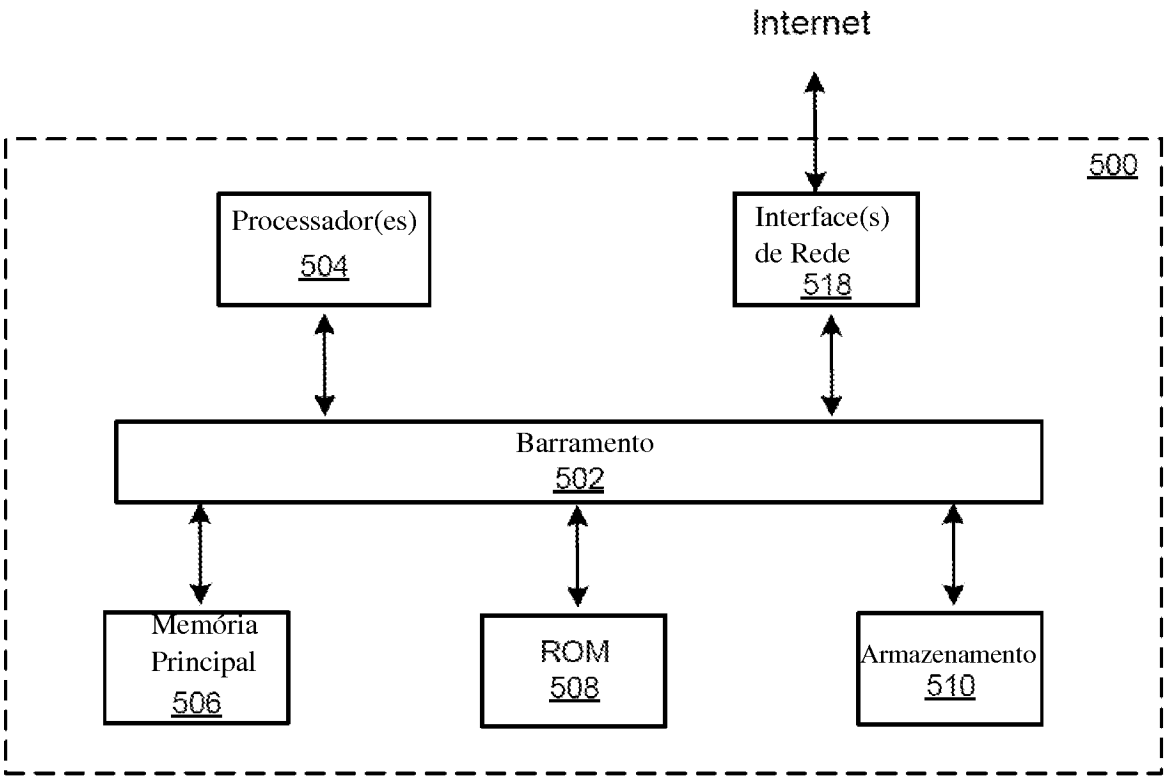

Internet
500
Processador(es)
504
Interface(s)
de Rede
518
Barramento
502
Memória
Principal
506
ROM
508
Armazenamento
510

FIG. 5

RESUMO

"SISTEMAS, MEIOS DE ARMAZENAMENTO E MÉTODOS PARA PROTEÇÃO DE INFORMAÇÕES"

Um método implementado por computador para proteção de informações compreende: comprometer um valor de transação de uma transação com um primeiro esquema de compromisso para obter um valor de compromisso de transação, comprometer uma alteração da transação com um segundo esquema de compromisso para obter um valor de compromisso de alteração, o primeiro esquema de compromisso compreendendo um fator de ocultação de transação, e o segundo esquema de compromisso compreendendo um fator de ocultação de alteração; criptografar uma primeira combinação do fator de ocultação de alteração e a alteração com uma primeira chave; transmitir o fator de ocultação de transação, o valor de transação, e o valor de compromisso de transação para um nó receptor associado a um receptor para o nó receptor verificar a transação; em resposta a isso, o receptor verifica com sucesso a transação, obter uma segunda combinação criptografada do fator de ocultação de transação e da quantidade de transação criptografada com uma segunda chave.