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

(21) BR 112019008168-2 A2

(22) Data do Depósito: 07/11/2018

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

(54) Título: MÉTODOS IMPLEMENTADOS POR COMPUTADOR, MEIO DE ARMAZENAMENTO LEGÍVEL POR COMPUTADOR E SISTEMA

(51) Int. Cl.: H04L 9/14.

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

(72) Inventor(es): ZHENG LIU; LICHUN LI; SHAN YIN.

(86) Pedido PCT: PCT CN2018114322 de 07/11/2018

(87) Publicação PCT: WO 2019/072262 de 18/04/2019

(85) Data da Fase Nacional: 22/04/2019

(57) Resumo: As formas de realização da presente invenção incluem a obtenção de uma chave secreta, através de um nó cliente (client node), de acordo com um esquema de compartilhamento secreto limiar acordado por uma pluralidade de nós clientes; gerar um ou mais valores de comprometimento de uma transação confidencial do nó cliente, através da aplicação de um esquema de comprometimento criptográfico aos dados de transação; gerar informação de transação criptografada da transação confidencial, através da criptografia dos dados de transação usando a chave secreta; e transmitir, a um nó de consenso de uma rede de protocolo de confiança (blockchain), um conteúdo da transação confidencial para execução, em que o conteúdo da transação confidencial compreende: o um ou mais valores de comprometimento; as informações de transação criptografadas; e uma ou mais provas de conhecimento zero dos dados de transação.

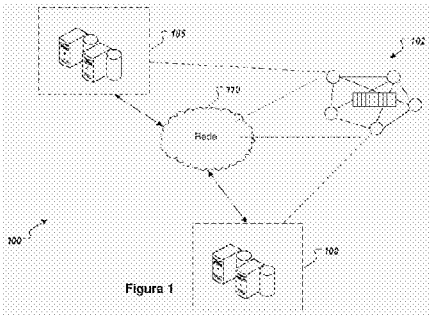

Figura 1

"MÉTODO IMPLEMENTADO POR COMPUTADOR DE UM NÓ CLIENTE PARTICIPANDO DE UMA TRANSAÇÃO CONFIDENCIAL DE PROTOCOLO DE CONFIANÇA, MÉTODO IMPLEMENTADO POR COMPUTADOR DE UM NÓ DE CONSENSO DE UMA REDE DE PROTOCOLO DE CONFIANÇA, MÉTODO IMPLEMENTADO POR COMPUTADOR PARA RECUPERAR INFORMAÇÕES DE TRANSAÇÕES CRIPTOGRAFADAS EM TRANSAÇÕES CONFIDENCIAIS DE PROTOCOLO DE CONFIANÇA, PRODUTO DE PROGRAMA DE COMPUTADOR E SISTEMA"

ANTECEDENTES DA INVENÇÃO

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

[002] Os protocolos de confiança são usados em redes de criptomoedas, que permitem aos participantes realizar transações para comprar/ vender mercadorias e/ ou serviços usando uma criptomoeda. Uma criptomoeda comum inclui o Bitcoin. Em redes de criptomoedas, os modelos de

manutenção de registros são usados para registrar transações entre usuários. Exemplos de modelos de manutenção de registos incluem um modelo de saldo de transação não realizada (UTXO), e o modelo de conta (também referido como modelo baseado em conta ou um modelo de conta/ saldo).

[003] No modelo UTXO, os ativos da cadeia estão na forma de transações. Cada transação gasta o saldo de transações anteriores e gera novos saldos que podem ser gastos em transações posteriores. As transações não gastas de um usuário são rastreadas e um saldo que o usuário deve gastar é calculado como a soma das transações não gastas. Cada transação leva em conta um ou mais saldos não gastos (e somente saldos não gastos) como entrada e pode ter um ou mais saldos. O requisito de que apenas os saldos não utilizados possam ser utilizados em outras transações é necessário para evitar gastos duplos e fraude. O modelo UTXO suporta a validação de transação e função à prova, mas o suporte para contratos inteligentes é fraco.

[004] O modelo de conta é adotado pela Ethereum. O modelo de conta executa manutenção de registros e gerencia saldos de contas como um banco tradicional. Sob este modelo, uma conta pode ter um endereço e um saldo da conta correspondente. Os ativos na cadeia são representados como o saldo da conta. Cada transação de transferência pode ter um endereço de conta de um ativo transferido e um endereço de conta de um ativo recebido. O valor da transação é diretamente atualizado no saldo da conta. O modelo de conta é eficiente, uma vez que cada transação pode precisar apenas validar que a conta de envio tem saldo suficiente para pagar a transação. Além de suportar a validação de transação e função de prova, o modelo de conta pode suportar totalmente contratos inteligentes, especialmente aqueles que exigem informações do estado ou envolvem várias partes.

DESCRIÇÃO RESUMIDA DA INVENÇÃO

[005] As formas de realização da presente invenção incluem

métodos implementados por computador para transações confidenciais com base em tecnologias de protocolo de confiança (referidas como transações confidenciais de protocolo de confiança ou, simplesmente, transações confidenciais). Mais particularmente, as formas de realização da presente invenção destinam-se a recuperar informações de transações criptografadas em transações confidenciais de protocolo de confiança.

[006] Em algumas formas de realização, as ações incluem a obtenção de uma chave secreta, através de um nó cliente (*client node*), de acordo com um esquema de compartilhamento secreto limiar acordado por uma pluralidade de nós clientes; gerar um ou mais valores de comprometimento de uma transação confidencial do nó cliente, através da aplicação de um esquema de comprometimento criptográfico aos dados de transação; gerar informação de transação criptografada da transação confidencial, através da criptografia dos dados de transação usando a chave secreta; e transmitir, a um nó de consenso de uma rede de protocolo de confiança, um conteúdo da transação confidencial para execução, em que o conteúdo da transação confidencial compreende: o um ou mais valores de comprometimento; as informações de transação criptografadas; e uma ou mais provas de conhecimento zero dos dados de transação.

[007] Em algumas formas de realização, as ações incluem receber um conteúdo de uma transação confidencial de um nó cliente, por um nó de consenso de uma rede de protocolo de confiança, em que o conteúdo da transação confidencial compreende: um ou mais valores de comprometimento da transação confidencial gerada pelo nó cliente, através da aplicação de um esquema de comprometimento criptográfico aos dados de transação da transação confidencial; e informação de transação criptografada gerada através da criptografia dos dados de transação usando uma chave secreta do nó cliente, em que uma chave secreta é obtida pelo nó cliente de acordo com um

esquema de compartilhamento secreto limiar com uma pluralidade de nós clientes; e uma ou mais provas de conhecimento zero dos dados de transação; verificar, através do nó de consenso da rede de protocolo de confiança, que a transação confidencial é válida com base no conteúdo da transação confidencial; e armazenar, através do nó de consenso da rede de protocolo de confiança, as informações de transação criptografadas em um protocolo de confiança da rede de protocolo de confiança.

[008] Em algumas formas de realização, as ações incluem receber, através de um nó cliente em particular de um nó de consenso de uma rede de protocolo de confiança, informações de transação criptografadas de uma transação confidencial do nó cliente em particular, em que as informações de transação criptografadas são armazenadas em pelo menos um protocolo de confiança na rede de protocolo de confiança, em que o nó cliente em particular não tem acesso a uma chave secreta configurada para descriptografar as informações de transação criptografada, e em que o nó cliente em particular foi anteriormente emitido a chave secreta; recuperar, através de um nó cliente em particular, a chave secreta através de pelo menos um número limiar de nó clientes entre uma pluralidade de nós clientes na rede de protocolo de confiança, de acordo com um esquema de compartilhamento secreto limiar, acordado pela pluralidade de nós clientes; e descriptografar, através do nó cliente em particular, dados de transação da transação confidencial do nó cliente em particular através das informações de transação criptografada usando a chave secreta recuperada.

[009] Outras formas de realização incluem sistemas, aparelhos e programas de computador correspondentes, configurados para executar as ações dos métodos, codificados em dispositivos de armazenamento de computador.

[010] Estas e outras formas de realização podem incluir,

opcionalmente, uma ou mais das seguintes características.

[011] Uma primeira característica, combinável com qualquer uma das seguintes características, em que os dados de transação da transação confidencial incluem um ou ambos os saldos de uma conta do nó cliente antes da transação confidencial ou um valor de transação da transação confidencial.

[012] Uma segunda característica, combinável com qualquer uma das características anteriores ou seguintes, em que a uma ou mais provas de conhecimento zero dos dados de transação inclui um ou mais intervalos de provas de conhecimento zero de que os valores dos dados de transação estão dentro dos respectivos intervalos.

[013] Uma terceira característica, combinável com qualquer uma das características anteriores ou seguintes, em que o esquema de comprometimento criptográfico inclui um esquema de comprometimento de Pedersen; em que gerar um ou mais valores de comprometimento de uma transação confidencial do nó cliente aplicando um esquema de comprometimento criptográfico a dados de transação inclui gerar um ou mais valores de comprometimento da transação confidencial do nó cliente com base nos dados da transação e números aleatórios correspondentes aos dados da transação; e em que a geração de informações de transação criptografadas da transação confidencial inclui a geração de informações de transação criptografadas da transação confidencial, criptografando os dados de transação e números aleatórios correspondentes aos dados de transação utilizando a chave secreta.

[014] Uma quarta característica, combinável com qualquer uma das características anteriores ou seguintes, em que esquema de compartilhamento secreto limiar compreende um esquema de compartilhamento secreto de Shamir.

[015] Uma quinta característica, combinável com qualquer uma

das características anteriores ou seguintes, em que verificar se a transação confidencial é válida com base no conteúdo da transação confidencial inclui: determinar que o um ou mais valores de comprometimento estejam corretos com base no esquema de comprometimento; e verificar as uma ou mais provas de conhecimento zero dos dados de transação.

[016] Uma sexta característica, combinável com qualquer uma das características anteriores ou seguintes, em que a verificação das uma ou mais provas de conhecimento zero dos dados de transação inclui: determinar que um saldo de conta do nó cliente antes da transação confidencial é maior que zero; e determinar que um valor de transação da transação confidencial é menor ou igual a um saldo de conta do nó cliente antes da transação confidencial.

[017] Uma sétima característica, combinável com qualquer uma das características anteriores ou seguintes, em que o esquema de comprometimento criptográfico é homomórfico, e o método compreende ainda a atualização de um saldo de conta do nó cliente após a transação confidencial com base no homomorfismo do esquema de comprometimento.

[018] Uma oitava característica, combinável com qualquer uma das características anteriores ou seguintes, em que descriptografar dados de transação da transação confidencial do nó cliente em particular, a partir da informação de transação criptografada utilizando a chave secreta inclui recuperar um valor de transferência da transação confidencial utilizando a chave secreta.

[019] Uma nona característica, combinável com qualquer uma das características anteriores ou seguintes, em que descriptografar dados de transação da transação confidencial do nó cliente em particular, a partir da informação de transação criptografada utilizando a chave secreta inclui recuperar tanto o valor de transferência da transação confidencial quanto um

número aleatório correspondente ao valor de transferência usando a chave secreta, em que o valor de transferência e o número aleatório são usados em um esquema de comprometimento de Pedersen para ocultar informações de transação da transação confidencial do nó cliente em particular.

[020] A presente invenção também fornece um ou mais meios de armazenamento legíveis por computador, não transitórios acoplados a um ou mais processadores e tendo instruções armazenadas no mesmo que, quando executado por um ou mais processadores, faz com que os um ou mais processadores execute as operações de acordo com formas de realização dos métodos aqui fornecidos.

[021] A presente invenção fornece ainda um sistema para implementar os métodos aqui fornecidos. O sistema inclui um ou mais processadores, e um produto de programa de computador acoplado a um ou mais processadores com instruções armazenadas nele que, quando executadas por um ou mais processadores, fazem com que um ou mais processadores executem operações de acordo com formas de realização. dos métodos aqui fornecidos.

[022] Entende-se que os métodos de acordo com a presente invenção podem incluir qualquer combinação dos aspectos e características aqui descritos. Isto é, métodos de acordo com a presente invenção não estão limitados às combinações de aspectos e características especificamente descritos aqui, mas também incluem qualquer combinação dos aspectos e características fornecidos.

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

BREVE DESCRIÇÃO DAS FIGURAS

[024] A Figura 1 ilustra um exemplo de ambiente que pode ser usado para executar as formas de realização da presente invenção.

[025] A Figura 2 ilustra um exemplo de arquitetura conceitual de acordo com as formas de realização da presente invenção.

[026] A Figura 3 ilustra um exemplo de processo 300 para preparar uma transação confidencial de protocolo de confiança de acordo com as formas de realização da presente invenção.

[027] A Figura 4 ilustra um exemplo de processo de recuperação (400) de informações de transação de uma transação confidencial de protocolo de confiança de acordo com as formas de realização da presente invenção.

[028] A Figura 5 ilustra um exemplo de processo que pode ser executado de acordo com as formas de realização da presente invenção.

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

DESCRIÇÃO DETALHADA DA INVENÇÃO

[030] As formas de realização da presente invenção incluem métodos implementados por computador para transações confidenciais com base em tecnologias de protocolo de confiança. Mais particularmente, as formas de realização da presente invenção destinam-se a recuperar informações de transações decodificadas em transações confidenciais de protocolo de confiança.

[031] Em algumas formas de realização, as ações incluem a obtenção de uma chave secreta, através de um nó cliente, de acordo com um esquema de compartilhamento secreto limiar acordado por uma pluralidade de nós clientes; gerar um ou mais valores de comprometimento de uma transação confidencial do nó cliente, através da aplicação de um esquema de comprometimento criptográfico aos dados de transação; gerar informação de

transação criptografada da transação confidencial, através da criptografia dos dados de transação usando a chave secreta; e transmitir, a um nó de consenso de uma rede de protocolo de confiança, um conteúdo da transação confidencial para execução, em que o conteúdo da transação confidencial inclui: o um ou mais valores de comprometimento; as informações de transação criptografadas; e uma ou mais provas de conhecimento zero dos dados de transação.

[032] Em algumas formas de realização, as ações incluem receber um conteúdo de uma transação confidencial de um nó cliente, por um nó de consenso de uma rede de protocolo de confiança, em que o conteúdo da transação confidencial inclui: um ou mais valores de comprometimento da transação confidencial gerada pelo nó cliente, através da aplicação de um esquema de comprometimento criptográfico aos dados de transação da transação confidencial; e informação de transação criptografada gerada através da criptografia dos dados de transação usando uma chave secreta do nó cliente, em que uma chave secreta é obtida pelo nó cliente de acordo com um esquema de compartilhamento secreto limiar com uma pluralidade de nós clientes; e uma ou mais provas de conhecimento zero dos dados de transação; verificar, através do nó de consenso da rede de protocolo de confiança, que a transação confidencial é válida com base no conteúdo da transação confidencial; e armazenar, através do nó de consenso da rede de protocolo de confiança, as informações de transação criptografadas em um protocolo de confiança da rede de protocolo de confiança.

[033] Em algumas formas de realização, as ações incluem receber, através de um nó cliente em particular de um nó de consenso de uma rede de protocolo de confiança, informações de transação criptografadas de uma transação confidencial do nó cliente em particular, em que as informações de transação criptografadas são armazenadas em pelo menos um protocolo de

confiança na rede de protocolo de confiança, em que o nó cliente em particular não tem acesso a uma chave secreta configurada para descriptografar as informações de transação criptografada, e em que o nó cliente em particular foi anteriormente emitido a chave secreta; recuperar, através de um nó cliente em particular, a chave secreta através de pelo menos um número limiar de nó clientes entre uma pluralidade de nós clientes na rede de protocolo de confiança, de acordo com um esquema de compartilhamento secreto limiar, acordado pela pluralidade de nós clientes; e descriptografar, através do nó cliente em particular, dados de transação da transação confidencial do nó cliente em particular através das informações de transação criptografada usando a chave secreta recuperada.

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

[035] Em uma rede de protocolo de confiança pública, o processo de consenso é controlado por nós da rede de consenso. Por exemplo, centenas, milhares, até mesmo milhões de entidades podem cooperar uma rede de protocolo de confiança pública, cada uma das quais opera pelo menos um nó na rede de protocolo de confiança pública. Assim, a

rede de protocolo de confiança pública pode ser considerada uma rede pública em relação às entidades participantes. Em alguns exemplos, a maioria das entidades (nós) deve assinar cada bloco, para que o bloco de ser válido, e adicionado ao protocolo de confiança (contabilidade distribuída) da rede de protocolo de confiança. Um exemplo de rede de protocolo de confiança pública inclui a rede de Bitcoin, que é uma rede de pagamento peer-to-peer. A rede de Bitcoin utiliza uma contabilidade distribuída, conhecida como protocolo de confiança. Como observado acima, o termo protocolo de confiança, no entanto, é usado para se referir geralmente a contabilidades distribuídas sem referência particular à rede de Bitcoin.

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

[037] Em geral, uma rede de protocolo de confiança privada é fornecida para uma entidade particular, que controla centralmente as permissões de leitura e gravação. A entidade controla quais nós são capazes de participar da rede de protocolo de confiança. Consequentemente, as redes de protocolo de confiança privadas são geralmente referidas como redes com permissão que colocam restrições sobre quem tem permissão para participar da rede, e sobre o seu nível de participação (por exemplo, apenas em certas

transações). Vários tipos de mecanismos de controle de acesso podem ser usados (por exemplo, os participantes existentes votam na adição de novas entidades, uma autoridade reguladora pode controlar a admissão).

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

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

[040] As formas de realização da presente invenção são aqui descritas em maior detalhe tendo em vista o contexto acima. Mais particularmente, e como apresentado acima, as formas de realização da presente invenção destinam-se a regular transações confidenciais de protocolo de confiança.

[041] Um protocolo de confiança é um registro digital compartilhado à prova de adulteração que registra transações em uma rede peer-to-peer pública ou privada. O registro é distribuído para todos os nós membros na rede e o histórico de transações de ativos ocorrendo na rede é permanentemente registrado no bloco. Como o registro é totalmente público para as entidades participantes, o registro de protocolo de confiança em si não tem função de proteção de privacidade e requer tecnologia adicional para proteger a privacidade do conteúdo da transação de ativos.

[042] As técnicas de proteção de privacidade para protocolo de confiança podem incluir aquelas para realizar uma transação confidencial para proteger a privacidade de um conteúdo de uma transação. Em uma transação confidencial, o conteúdo de uma transação só é acessível ou conhecido pelos participantes da transação, e não por outros estranhos. Por exemplo, uma transação confidencial permite apenas que as duas partes participando da transação estejam a par do montante a ser transacionado, e observadores externos são impedidos de saber esta informação. Tais técnicas para realizar transações confidenciais foram usadas, por exemplo, em MONERO e ZCASH.

[043] Técnicas de proteção de privacidade para protocolo de confiança também podem incluir aquelas para proteger identidades de partes de uma transação, como, por exemplo, usando um endereço invisível ou um mecanismo de assinatura de anel.

[044] Com a proteção de privacidade adicionada ao protocolo de confiança (por exemplo, no contexto de transações confidenciais), um esquema de comprometimento, como o esquema de comprometimento de Pedersen, pode ser usado para ocultar ou criptografar determinadas informações de transação de um nó cliente. As informações da transação podem incluir, por exemplo, o saldo da conta de um usuário antes da transação, um valor de transação e/ ou outras informações. Por exemplo, um nó cliente (também

chamado de cliente, usuário, parte ou participante da transação) pode prometer ou comprometer-se com um saldo de conta pré-transação α e um número aleatório correspondente r de acordo com o esquema de comprometimento de Pedersen. O nó cliente pode salvar o valor α e o número aleatório r. Quando α ou r correspondente ao comprometimento é perdido, o saldo na conta não pode ser usado pelo nó cliente. Por exemplo, em um caso em que ambos α e r são perdidos, o nó cliente não conhece o saldo a nem o número aleatório r correspondente ao saldo. Em um caso em que apenas r, mas não α, é perdido, o nó cliente pode conhecer o saldo t, mas não pode usar seu próprio saldo, porque o uso do saldo envolve operações de r. Em um caso em que α é perdido, o cliente não conhece seu próprio saldo. O nó cliente não pode restaurar ou recuperar a quantidade de texto sem formatação α se o poder de computação do nó cliente for limitado.

[045] Exemplos de técnicas são descritas para resolver o problema acima descrito quando um esquema de comprometimento (por exemplo, o comprometimento de Pedersen) é usado para ocultar ou criptografar informações de uma transação. As técnicas descritas podem tornar possível e mais fácil para um nó cliente recuperar as informações originais da transação de texto simples (por exemplo, o valor comprometido α e/ ou o número aleatório r) no caso em que tais informações de transação são perdidas.

[046] As técnicas descritas incluem um esquema de recuperação para recuperar informações de transação ocultas (por exemplo, um valor de transação comprometido que foi perdido) em transações confidenciais de protocolo de confiança. Em algumas formas de realização, as técnicas descritas incluem armazenar as informações de transação ocultas em um ou mais protocolo de confianças em uma rede de protocolo de confiança. Em algumas formas de realização, as informações de transação ocultas de uma

transação confidencial armazenada no protocolo de confiança podem ser criptografadas. As informações antes da criptografia podem ser chamadas de informações de texto sem formatação. As informações resultantes após a criptografia podem ser chamadas de informações criptografadas ou de texto cifrado.

[047] Em algumas formas de realização, um nó cliente pode criptografar certos dados de transação (ou seja, dados de transação de texto sem formatação) em dados de transação criptografados ou de texto cifrado usando uma chave secreta. Por exemplo, um nó cliente pode criptografar tanto um valor de texto simples (por exemplo, as informações da conta) quanto um número aleatório correspondente ao valor de texto simples de acordo com o comprometimento de Pedersen usando uma chave secreta. As informações de transação criptografadas resultantes da transação confidencial (por exemplo, o número aleatório criptografado e o valor de texto simples criptografado) podem ser incluídas como parte de um conteúdo da transação e enviadas para execução pela rede de protocolo de confiança. Um ou mais nós de protocolo de confiança podem armazenar as informações da transação criptografada, por exemplo, em um ou mais protocolo de confianças na rede de protocolo de confiança. O nó cliente pode recuperar as informações de transação criptografadas correspondentes ao nó cliente a partir de um ou mais nós de protocolo de confiança e descriptografar os dados de transação de texto sem formatação das informações da transação criptografada usando a chave secreta.

[048] Em algumas formas de realização, o nó cliente pode perder os dados de transação de texto sem formatação e/ ou a chave secreta. Por exemplo, se o nó cliente salvou os dados de transação de texto sem formatação e/ ou a chave secreta localmente, em um armazenamento de dados do nó cliente, o nó cliente poderá perder os dados de transação de texto

sem formatação e/ ou a chave secreta quando o armazenamento de dados estiver compreendido ou danificado. As técnicas descritas podem ajudar a recuperar os dados de transação de texto simples e/ ou a chave secreta.

[049] Em algumas formas de realização, a chave secreta do nó cliente pode ser gerada de acordo com um esquema de compartilhamento secreto limiar (por exemplo, o esquema de compartilhamento secreto de Shamir) para o cálculo seguro de múltiplas partes (MPC). Por exemplo, uma chave secreta privada correspondente ao comprometimento de criptografia do nó cliente pode ser negociada e gerada entre um número total de participantes (por exemplo, n participantes) do esquema de compartilhamento secreto de Shamir. A chave secreta pode ser dividida em várias partes e armazenada pelo número total de participantes, respectivamente, evitando assim o vazamento da chave secreta do nó cliente. No caso em que o nó cliente perde a chave secreta, o nó cliente pode recuperar a chave secreta de acordo com o esquema de compartilhamento secreto de Shamir, recebendo pelo menos um número limite de partes (por exemplo, k partes) da chave secreta de pelo menos k de n participantes. Consequentemente, o nó cliente pode recuperar a chave secreta e usar a chave secreta para descriptografar os dados de transação de texto simples a partir das informações da transação criptografada usando a chave secreta.

[050] As técnicas descritas podem ajudar a recuperar a chave secreta e os dados de transação de texto simples de uma transação confidencial. As técnicas descritas não dependem de um esquema de backup com base em hardware, no qual nós clientes usam seu hardware para fazer backup de suas chaves secretas (por exemplo, em carteiras com base em hardware). As técnicas descritas podem fornecer segurança e robustez aprimoradas dos dados de transação, pois os dados de transação são armazenados em um ou mais protocolo de confiança na rede de protocolo de

confiança. As técnicas descritas podem fornecer acesso a um nó cliente para sua chave secreta, independentemente de uma forma de realização de uma carteira com base em hardware ou de uma carteira com base em software. As técnicas descritas podem alcançar vantagens adicionais ou diferentes.

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

[052] No exemplo descrito, os sistemas de computação (106, 108) podem incluir qualquer sistema de computação apropriado que permita a participação como um nó na rede de protocolo de confiança de consórcio (102). Exemplos de dispositivos de computação incluem, sem limitação, um servidor, um computador de mesa, um computador laptop, um dispositivo de computador de tablet e um smartphone. Em alguns exemplos, os sistemas de computação (106, 108) hospedam um ou mais serviços implementados por computador para interagir com a rede de protocolo de confiança de consórcio (102). Por exemplo, o sistema de computação (106) pode hospedar serviços implementados por computador de uma primeira entidade (por exemplo, cliente A), tal como um sistema de gerenciamento de transações que a primeira entidade usa para gerenciar suas transações com uma ou mais entidades (por exemplo, outros clientes). O sistema de computação (108) pode hospedar

serviços implementados por computador de uma segunda entidade (por exemplo, cliente B), tal como o sistema de gerenciamento de transação que a segunda entidade usa para gerenciar suas transações com uma ou mais outras entidades (por exemplo, outros clientes). No exemplo da Figura 1, a rede de protocolo de confiança de consórcio (102) é representada como uma rede peer-to-peer de nós, e os sistemas de computação (106, 108) fornecem nós da primeira entidade e segunda entidade, respectivamente, que participam na rede de protocolo de confiança de consórcio (102).

[053] A Figura 2 ilustra um exemplo de arquitetura conceptual (200) de acordo com formas de realização da presente invenção. A arquitetura conceitual exemplificativa (200) inclui uma camada de entidade (202), uma camada de serviços hospedados (204) e uma camada de rede de protocolo de confiança (206). No exemplo representado, a camada de entidade (202) inclui três entidades, Entidade_1 (E1), Entidade_2 (E2) e Entidade_3 (E3), cada entidade possuindo um respectivo sistema de gestão de transações (208).

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

exemplos, as interfaces (210) “hospedam” os nós de rede de protocolo de confiança para os respectivos sistemas de gestão de transação (208). Por exemplo, as interfaces (210) fornecem a interface de programação de aplicativos (API) para acessar a rede de protocolo de confiança (212).

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

[056] A Figura 3 ilustra um exemplo de processo (300) para preparar uma transação confidencial de acordo com formas de realização da presente invenção. Os nós clientes A (302), B (304), C (306) e D (308) representam participantes de um esquema de compartilhamento secreto limiar (também chamado de esquema de compartilhamento de chave limiar). Um esquema de compartilhamento limiar limita o problema do gerenciamento de chave de segurança por várias partes. Como um exemplo de esquema de compartilhamento secreto, o esquema de compartilhamento secreto de Shamir (denotado como Shamir (k, n)) divide uma chave secreta em n partes e atribui as n partes a n participantes, respectivamente. Cada participante tem uma parte única da chave secreta. Para reconstruir a chave secreta original, é necessário um número mínimo ou limiar de peças. No esquema limiar, esse número mínimo, k, é menor que o número total de partes, n. Em outras

palavras, a chave secreta original pode ser recuperada se pelo menos k partes da chave secreta forem coletadas. O algoritmo de Shamir pode usar, por exemplo, um algoritmo de diferença lagrangiana ou outros métodos para recuperar a chave secreta.

[057] Aqui, Shamir (k, n) significa que um texto simples m é criptografado e dividido em n partes, e pelo menos k partes são necessárias para recuperar o texto simples m. Como mostrado na Figura 3, o nó cliente A (302) pode gerar uma chave, Achave, e decompor a Achave em quatro partes. O nó cliente A (302) pode manter uma parte e fornecer uma parte respectiva para cada nó cliente B (304), C (306) e D (308).

[058] Em algumas formas de realização, a partir da perspectiva do nó cliente A (302), em (310), o nó cliente A (302) pode negociar e obter uma chave secreta, Achave, de acordo com o esquema de compartilhamento secreto de Shamir, denotado como Shamir (k, n), como descrito acima. Os valores de k e n podem ser determinados, por exemplo, pelo nó cliente A (302) ou outra parte com base em considerações de segurança e complexidade. No exemplo mostrado na Figura 3, n poderia ser 4 para que os nós clientes A (302), B (304), C (306) e D (308) fossem todos participantes do esquema de compartilhamento secreto de Shamir. Nesse caso, k pode ser 2 ou 3 para que o nó cliente A (302) possa recuperar a chave secreta, Achave, de pelo menos 2 ou 3 participantes de todos os participantes, nós clientes A (302), B (304), C (306) e D (308). Como outro exemplo, k poderia ser 4 e n poderia ser maior que 4 para que o nó cliente A (302) pudesse recuperar a chave secreta, Achave, de pelo menos 4 participantes de todos os participantes do esquema de compartilhamento secreto de Shamir.

[059] Em algumas formas de realização, o nó cliente A (302) é um exemplo dos sistemas de computação (106, 108) correspondendo a um primeiro cliente ou entidade, como descrito nas Figuras 1 e 2. O nó cliente A

(302) tem uma conta correspondente (por exemplo, uma conta pública ou uma conta privada) para transações através de uma rede de protocolo de confiança (350). A rede de protocolo de confiança (350) pode incluir múltiplos nós de consenso (tais como nós de protocolo de confiança (312) na Figura 3). Em algumas formas de realização, os nós clientes B (304), C (306) e D (308) podem ou não ser nós cliente da rede de protocolo de confiança (350). Em outras palavras, o nó cliente A (302) pode obter a chave secreta independentemente da rede de protocolo de confiança (350). Por exemplo, o nó cliente A (302) pode obter a chave secreta dos nós clientes B (304), C (306) e D (308) através de comunicações da rede de protocolo de confiança (350).

[060] Em algumas formas de realização, o nó cliente A (302) pode realizar uma transação confidencial com outro nó cliente (por exemplo, um nó cliente B (304)) de forma que as informações da transação sejam visíveis ou conhecidas pelo nó cliente A (302) e nó cliente B (304), mas não outras partes (por exemplo, o nó cliente C (306) ou D (308), ou os nós de protocolo de confiança (312) na rede de protocolo de confiança (350)).

[061] Em (320), o nó cliente A (302) cria uma transação confidencial para transferir uma quantia t para o nó cliente B (304). Em algumas formas de realização, o nó cliente A (302) pode construir um conteúdo da transação confidencial localmente e enviar o conteúdo da transação confidencial para a rede de protocolo de confiança (350) (por exemplo, um ou mais nós de protocolo de confiança (312) na rede de protocolo de confiança (350)).

[062] Em algumas formas de realização, a transação confidencial pode ser construída com base em um esquema de comprometimento para ocultar os dados da transação (por exemplo, o saldo da conta antes da transação e o valor da transação). Um exemplo de esquema de comprometimento inclui, sem limitação, o comprometimento de Pedersen (PC).

Por exemplo, o nó cliente A (302) gera um valor de comprometimento com base em um valor da transação t e um número aleatório r usando o PC. Por exemplo, o valor de comprometimento inclui um texto cifrado que pode ser obtido de acordo com PC (t) = rG + tH, onde G e H podem ser geradores de uma curva elíptica, PC (t) é uma multiplicação escalar de pontos de curva, t é o valor que está comprometido. O esquema de comprometimento de PC tem um homomorfismo, ou seja, PC (t_1) + PC (t_2) = PC (t_1 + t_2). Os titulares do texto cifrado PC (t) podem verificar o valor da transação t usando o número aleatório r. Embora as formas de realização da presente divulgação sejam aqui descritas em maior detalhe com referência ao PC, é contemplado que as formas de realização da presente divulgação possam ser realizadas utilizando qualquer esquema de comprometimento apropriado.

[063] No exemplo de transação confidencial, o nó cliente A (302) pode comprometer-se a um saldo da conta pré-transação a e um montante de transferência t. Em algumas formas de realização, o nó cliente A (302) pode gerar um valor de comprometimento PC (a) usando um PC baseado no saldo da conta pré-transação a e um número aleatório correspondente ra. Da mesma forma, o nó cliente A (302) pode gerar um valor de comprometimento PC (t) usando o PC com base no saldo de conta pré-transação a e um número aleatório correspondente rt. Em algumas formas de realização, nó cliente A (302) também pode comprometer que ele tem fundos suficientes para que o equilíbrio pós-transação a - t seja maior ou igual a 0. Por exemplo, nó cliente A (302) pode gerar um valor de comprometimento PC (a- t), por exemplo, com base nos valores de comprometimento PC (a) e PC (t), homomórfico propriedade do PC. Os valores de comprometimento podem ser incluídos no conteúdo da transação confidencial.

[064] Em algumas formas de realização, o conteúdo da transação confidencial pode incluir uma ou mais provas de conhecimento zero

para permitir que uma parte receptora confirme que a informação da parte remetente está enviando é válido. A prova de conhecimento zero permite que a parte receptora faça isso sem conhecimento real da informação a ser confirmada. As provas de conhecimento zero podem incluir prova de intervalo, como Prova (a > 0), Prova (t > 0) e Prova (a > 0), ou outros tipos de prova. As provas de conhecimento zero permitem que a parte receptora (por exemplo, nó cliente B) confirme que a parte remetente (por exemplo, nó cliente A) tem fundos suficientes para transferir (ou seja, a - t > 0) e que o valor da transferência é maior que zero, sem saber o saldo a partir do qual o montante está sendo transferido, ou mesmo o valor da transferência t.

[065] Em algumas formas de realização, para cada comprometimento de Pedersen, o número aleatório r e quantidade t podem ser criptografados usando a chave secreta, Achave, para obter as informações de transação criptografadas, M = Achave (r, t). A informação de transação criptografada M pode ser incluída como parte do conteúdo da transação confidencial.

[066] Em algumas formas de realização, o conteúdo do exemplo de transação confidencial pode incluir outras informações relacionadas à transação, como a assinatura digital de A na transação.

[067] Após gerar o conteúdo da transação, o nó cliente A (302) pode enviar o conteúdo da transação confidencial para a rede de protocolo de confiança (350) (por exemplo, um ou mais nós de protocolo de confiança (312) na rede de protocolo de confiança (350)). Em (330), a rede de protocolo de confiança (350) pode executar a transação confidencial. Em algumas formas de realização, a transação confidencial pode ser executada por cada um dos nós de protocolo de confiança (312) na rede de protocolo de confiança (350). Por exemplo, cada um dos nós de protocolo de confiança (312) pode determinar se o conteúdo da transação confidencial é legítimo, por exemplo, verificando um

ou mais valores de omissão e provas de conhecimento zero incluídas no conteúdo da transação confidencial. Por exemplo, cada um dos nós de protocolo de confiança (312) pode verificar os valores de comprometimento por verificação PC (a) = PC (t) + PC (a - t), que é, valores de transação de entrada é igual aos valores de transação de saldo. Cada um dos nós de protocolo de confiança (312) pode verificar as provas de conhecimento zero, por exemplo, com base em prova de balas (*Bulletproofs*), algoritmos RingCT da Monero ou quaisquer outros algoritmos adequados.

[068] Em algumas formas de realização, após os valores de comprometimento e provas de conhecimento zero serem verificados, cada um dos nós de protocolo de confiança (312) pode registrar a transação e atualizar as contas do nó cliente A (302) e nó cliente B (304). Por exemplo, após a transação, o nó cliente A (302) possui um saldo de conta a - t e o nó cliente B (304) possui um saldo de n b + t. Em algumas formas de realização, o saldo pós-transação do nó cliente A (302) e do nó cliente B (304) pode ser refletido pelas operações diretas do valor de comprometimento devido ao homomorfismo do esquema de confirmação. Por exemplo, o nó cliente A (302) agora pode ter um valor de comprometimento de um saldo de conta pós-transação PC (a -t) = PC (a) - PC (t). O nó cliente B (304) agora pode ter um valor de comprometimento de um saldo de conta pós-transação PC (b + t) = PC (b) + PC (t).

[069] Em algumas formas de realização, cada um dos nós de protocolo de confiança (312) pode gravar ou armazenar as informações da transação criptografada. Por exemplo, as informações de transação criptografadas correspondentes ao comprometimento PC (a), Ma = Achave (ra, a) e as informações de transação criptografadas correspondentes ao comprometimento PC (t), Mt = Achave (rt, t) podem ser registradas no protocolo de confiança por cada nó de protocolo de confiança (312), em que ra e rt

representam números aleatórios correspondendo à quantidade a e t, respectivamente.

[070] A Figura 4 representa um exemplo de processo de recuperação (400) de informações de transação de uma transação confidencial de acordo com formas de realização da presente invenção. Por exemplo, em um caso em que o nó cliente A (302) perde sua chave, Achave, e, portanto, não sabe o valor em sua conta de protocolo de confiança correspondente. O nó cliente A (302) pode utilizar o processo de recuperação de exemplo (400) para recuperar o valor da conta do nó cliente A (302).

[071] Em (410), o nó cliente A (302) obtém as informações de transação criptografadas sob o comprometimento de Pedersen (por exemplo, Ma = Achave (ra, a) e Mt = Achave (rt, t)), por exemplo, baixando ou sincronizando com o nó de protocolo de confiança (312). Em algumas formas de realização, o nó cliente A (302) pode salvar uma cópia local das informações da transação criptografada sob o comprometimento de Pedersen.

[072] Em (420), o nó cliente A (302) pode comunicar com os nós clientes B (304), C (306) e D (308), por exemplo, para recuperar a chave, Achave, de acordo com o esquema de comprometimento secreto de Shamir, por exemplo, da rede de protocolo de confiança (350).

[073] Com a chave recuperada, Achave, em (430), o nó cliente A (302) pode descriptografar as informações de transação criptografadas correspondentes a cada comprometimento de Pedersen da conta do nó cliente (302) (por exemplo, Ma = Achave (ra, a) e Mt = Achave (rt, t)). Em seguida, o nó cliente A (302) pode descriptografar as informações da transação criptografada (por exemplo, Ma = Achave (ra, a) e Mt = Achave (rt, t)) usando a chave recuperada, Achave e obter as informações da transação de texto simples ra, a, rt, e T.

[074] A Figura 5 ilustra um exemplo de processo (500) que pode

ser executado em conformidade com as formas de realização da presente invenção. Em algumas formas de realização, o exemplo de processo (500) pode ser executado usando um ou mais programas executáveis por computador executados usando um ou mais dispositivos de computação. Para clareza de apresentação, a descrição que se segue geralmente descreve o método (500) no contexto das outras figuras nesta descrição. Por exemplo, o nó cliente (510) pode incluir o nó cliente C (306) e o nó cliente D (308), o nó de protocolo de confiança (520) pode ser o nó de protocolo de confiança (312), o nó cliente A (530) pode ser o nó cliente A (302), e o nó cliente B (540) pode ser o nó cliente B (304) como descrito em relação às Figuras 3 e 4. No entanto, será entendido que o método (500) pode ser executado, por exemplo, por qualquer sistema, ambiente, software e hardware adequados, ou uma combinação de sistemas, ambientes, software e hardware, conforme apropriado. Em algumas formas de realização, várias etapas do método (500) podem ser executadas em paralelo, em combinação, em loops ou em qualquer ordem.

[075] Em (512), um número de nós cliente (por exemplo, n) (510) gera uma chave secreta para um nó cliente (por exemplo, nó cliente A (530)) de uma rede de protocolo de confiança. Em algumas formas de realização, a chave secreta pode ser negociada ou gerada por um número total de (por exemplo, n) nós clientes (510) de acordo com um esquema de compartilhamento limiar acordado pelo número total de nós clientes (510). Em algumas formas de realização, o esquema de compartilhamento secreto limiar compreende o esquema de compartilhamento secreto de Shamir.

[076] No número (514), o número de nós clientes (510) pode emitir a chave secreta para o nó cliente A (530). A chave secreta pode ser usada pelo nó cliente A (530) para criptografar e descriptografar informações de transação de uma transação confidencial do nó cliente A (530).

[077] Em (532), o nó cliente A (530) obtém a chave secreta de acordo com um esquema de comprometimento secreto limiar acordado com o número total de nós clientes (510) (por exemplo, o número total de participantes do esquema de comprometimento secreto). O nó cliente A (530) pode usar a chave secreta do nó cliente A (530) para criptografar dados de transação de uma transação confidencial do nó cliente A (530). A transação confidencial do nó cliente A (530) pode ser, por exemplo, uma transação confidencial (535) como a transferência de uma quantia de fundos de uma conta do nó cliente A (530) para uma conta do nó cliente B 540. O nó cliente A (530) pode construir um conteúdo da transação confidencial para proteger a privacidade dos dados de transação e ocultar os dados de transação sejam inspecionados por outras entidades, exceto os participantes da transação (isto é, o nó cliente A (530) e o nó cliente B (540) neste exemplo). Em algumas formas de realização, o nó cliente A (530) pode ocultar os dados de transação da transação confidencial com base em um esquema de comprometimento e usando a chave secreta obtida de acordo com o esquema de compartilhamento secreto limiar.

[078] Em algumas formas de realização, os dados de transação da transação confidencial compreendem um ou ambos os saldos de uma conta do nó cliente A (530) antes da transação confidencial ou um valor de transação da transação confidencial. Em algumas formas de realização, os dados da transação da transação confidencial podem incluir informações adicionais de transação (por exemplo, data da transação, as partes da transação, tipo de ativo (por exemplo, a segurança de ações ou um outro tipo)).

[079] Em (534), o nó do cliente A (530) gera um ou mais valores de comprometimento da transação confidencial do nó do cliente A (530) aplicando um esquema de comprometimento criptográfico aos dados de transação da transação confidencial. Em algumas formas de realização, o

esquema de comprometimento criptográfico compreende um esquema de comprometimento criptográfico homomórfico, tal como, um esquema de comprometimento de Pedersen, ou outro tipo de esquema de comprometimento.

[080] Em 536, o nó cliente A (530) gera informações de transação criptografadas da transação confidencial criptografando os dados da transação usando a chave secreta do nó cliente A (530), em que as informações de transação criptografadas estão configuradas para permitir a descriptografia pelo nó cliente A (530) usando a chave secreta.

[081] Em algumas formas de realização, o esquema de comprometimento criptográfico compreende o esquema de comprometimento de Pedersen. Neste caso, gerar um ou mais valores de comprometimento de uma transação confidencial do nó do cliente pela aplicação de um esquema de comprometimento criptográfico aos dados da transação compreende gerar um ou mais valores de comprometimento da transação confidencial do nó do cliente com base em os dados da transação e números aleatórios correspondentes aos dados da transação; e gerar informações de transação criptografadas da transação confidencial compreende gerar informações de transação criptografadas da transação confidencial através da criptografia dos dados de transação e números aleatórios correspondentes aos dados de transação usando a chave secreta do nó cliente A (530).

[082] Em (538), o nó cliente A (530) envia o conteúdo da transação confidencial à rede de protocolo de confiança para execução, por exemplo, transmitindo o conteúdo da transação confidencial para o nó de protocolo de confiança (520) (por exemplo, um nó de consenso da rede de protocolo de confiança). Em algumas formas de realização, o conteúdo da transação confidencial pode incluir: os um ou mais valores de comprometimento da transação confidencial gerados pelo nó cliente A (530),

aplicando o esquema de comprometimento criptográfico aos dados de transação da transação confidencial; as informações de transação criptografadas geradas pelo nó cliente A (530), criptografando os dados da transação usando a chave secreta; e uma ou mais provas de conhecimento zero dos dados da transação.

[083] Em algumas formas de realização, uma ou mais provas de conhecimento zero dos dados de transação, compreende um ou mais intervalos de provas de conhecimento zero, de que os valores dos dados da transação estão dentro dos respectivos intervalos. Por exemplo, os um ou mais intervalos de provas de conhecimento zero podem incluir um intervalo de prova de conhecimento zero de que o saldo da conta do nó cliente A (530) antes da transação confidencial é maior que zero, um intervalo de prova de conhecimento zero de que a quantia de transação da transação confidencial é maior que zero, e um intervalo de prova de conhecimento zero de que o montante da transação é inferior ou igual ao saldo da conta do nó cliente A (530) antes que a transação confidencial.

[084] Em algumas formas de realização, o conteúdo da transação confidencial compreende ainda uma assinatura digital do nó cliente A (530). Em algumas formas de realização, o conteúdo da transação confidencial pode incluir informações adicionais ou diferentes.

[085] Em (522), ao receber o conteúdo da transação confidencial, o nó de protocolo de confiança (520) pode executar a transação confidencial, por exemplo, verificando que a transação confidencial é válida com base no conteúdo da transação confidencial. Em algumas formas de realização, a verificação de que a transação confidencial é válida com base no conteúdo da transação confidencial pode incluir uma ou mais das seguintes: determinar que um ou mais valores de comprometimento estão corretos com base no esquema de comprometimento e/ ou em uma ou mais provas de conhecimento zero; ou

verificar se uma ou mais provas de conhecimento zero dos dados de transações, por exemplo, de acordo com algoritmos como descritos em relação à Figura 3.

[086] Em (524), após verificar que a transação confidencial é válida, o nó de protocolo de confiança (520) pode atualizar as informações da conta efetuadas pela transação confidencial (por exemplo, o saldo da conta do nó cliente A (530) e do nó cliente B (540). Em algumas formas de realização, o esquema de comprometimento criptográfico é homomórfico, e o nó de protocolo de confiança (520) pode atualizar informações de conta com base no homomorfismo do esquema de comprometimento, por exemplo, de acordo com as técnicas descritas com relação à Figura 3 ou outras técnicas.

[087] No (526), o nó de protocolo de confiança (520) pode armazenar as informações de transação criptografadas em um protocolo de confiança da rede de protocolo de confiança. Em algumas formas de realização, as informações de transação criptografadas podem ser armazenadas em mais de um/ todos os nós de consenso da rede de protocolo de confiança, fornecendo assim um backup robusto das informações de transação criptografadas do nó cliente A (530) caso o nó cliente A (530) perca a chave secreta. Além disso, o armazenamento das informações de transação criptografadas no protocolo de confiança da rede de protocolo de confiança pode reduzir ou eliminar a dependência do nó cliente A (530) em um esquema de armazenamento local ou de ponto único, melhorando a segurança e a confiabilidade do acesso do nó cliente A (530) às informações de transação criptografadas.

[088] No (528), o nó cliente A (530) pode recuperar ou, de outro modo, obter as informações de transação criptografadas do nó de protocolo de confiança (520) (por exemplo, um nó de consenso da rede de protocolo de confiança). As informações de transação criptografadas são armazenadas em

pelo menos um protocolo de confiança na rede de protocolo de confiança. O nó cliente A (530) pode descriptografar as informações da transação de texto simples a partir das informações da transação criptografada usando a chave secreta.

[089] Em (542), o nó cliente A (530) determina que perde ou não tem acesso à chave secreta configurada para descriptografar as informações da transação criptografada, e a chave secreta foi previamente emitida para o nó cliente A (530).

[090] Em (544), em algumas formas de realização, em resposta a tal determinação, o nó cliente A (530) recupera a chave secreta de pelo menos um número limite (por exemplo, k) de nós clientes entre um número total (por exemplo, n) de nós cliente a rede de protocolo de confiança, de acordo com um esquema de compartilhamento secreto limiar (por exemplo, o esquema de compartilhamento secreto de Shamir) aceito pela pluralidade de nós clientes, por exemplo, recebendo pelo menos o número limite de partes da chave secreta de pelo menos o número limite de nós clientes entre o número total de nós clientes na rede de protocolo de confiança.

[091] Em (546), o nó cliente A (530) descriptografa dados de transação (por exemplo, dados de transação de texto simples) da transação confidencial do nó cliente A (530) da informação de transação criptografada utilizando a chave secreta recuperada. Em algumas formas de realização, a descriptografia de dados de transação da transação confidencial do nó cliente em particular a partir das informações de transação criptografada usando a chave secreta compreende a recuperação de uma quantia de transferência da transação confidencial usando a chave secreta. Em algumas formas de realização, descriptografar dados de transação da transação confidencial do nó cliente em particular da informação de transação criptografada usando a chave secreta compreende a recuperação de uma quantidade de transferência da

transação confidencial e um número aleatório correspondente à quantia de transferência usando a chave secreta, o valor de transferência e o número aleatório são usados em um esquema de comprometimento de Pedersen para ocultar informações de transação da transação confidencial do nó cliente em particular.

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

[093] Processadores adequados para a realização de um

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

[094] Para fornecer a interação com um cliente, as características podem ser implementadas em um computador com um dispositivo de exibição, como um monitor de tubo de raio catódico (CRT) ou de cristal líquido (LCD) para exibir informações ao nó cliente A (302), um teclado e um dispositivo apontador, como um mouse ou uma *trackball*, pelos quais o cliente pode fornecer entrada para o computador.

[095] As características podem ser implementadas em um sistema de computador que inclua um componente de painel administrativo (back-end), como um servidor de dados, ou que inclua um componente de

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

[096] O sistema de computador pode incluir clientes e servidores. Um nó cliente A (302) e servidor geralmente são remotos entre si e geralmente interagem através de uma rede, como a descrita. A relação de nó cliente A (302) e servidor surge em virtude de programas de computador em realização nos respectivos computadores e tendo um relacionamento cliente-servidor entre si.

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

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

REIVINDICAÇÕES

1. MÉTODO IMPLEMENTADO POR COMPUTADOR DE UM NÓ CLIENTE (302, 530, 304, 540, 306, 308) PARTICIPANDO DE UMA TRANSAÇÃO CONFIDENCIAL (535) DE PROTOCOLO DE CONFIANÇA, o método caracterizado pelo fato de que compreende:

obtenção de uma chave secreta, através de um nó cliente (302, 530, 304, 540, 306, 308), de acordo com um esquema de compartilhamento secreto limiar acordado por uma pluralidade de nós clientes (302, 530, 304, 540, 306, 308);

gerar um ou mais valores de comprometimento de uma transação confidencial (535) do nó cliente (302, 530, 304, 540, 306, 308), através da aplicação de um esquema de comprometimento criptográfico aos dados de transação;

gerar informação de transação criptografada da transação confidencial (535), através da criptografia dos dados de transação usando a chave secreta; e

transmitir, a um nó de consenso de uma rede de protocolo de confiança (312, 520), um conteúdo da transação confidencial (535) para execução, em que o conteúdo da transação confidencial (535) compreende:

- o um ou mais valores de comprometimento;

- as informações de transação criptografadas; e

- uma ou mais provas de conhecimento zero dos dados de transação.

2. MÉTODO, de acordo com a reivindicação 1, caracterizado pelo fato de que os dados de transação da transação confidencial (535) compreendem um ou ambos dos saldos da conta do nó cliente (302, 530, 304, 540, 306, 308) antes da transação confidencial (535) ou um valor de transação da transação confidencial (535).

3. MÉTODO, de acordo com a reivindicação 1, caracterizado pelo fato de que uma ou mais provas de conhecimento zero dos dados de transação compreende um ou mais intervalos de provas de conhecimento zero de que os valores dos dados de transação estão dentro dos respectivos intervalos.

4. MÉTODO, de acordo com a reivindicação 1, caracterizado pelo fato de que:

o esquema de comprometimento criptográfico compreende um esquema de comprometimento de Pedersen;

em que gerar um ou mais valores de comprometimento de uma transação confidencial (535) do nó cliente (302, 530, 304, 540, 306, 308) através da aplicação de um esquema de comprometimento criptográfico aos dados de transação compreende gerar um ou mais valores de comprometimento da transação confidencial (535) do nó cliente (302, 530, 304, 540, 306, 308) com base nos dados de transação e números aleatórios correspondentes aos dados de transação; e

em que a geração de informação de transação criptografada da transação confidencial (535) compreende gerar informação de transação criptografada da transação confidencial (535) através da criptografia dos dados de transação e números aleatórios correspondentes aos dados de transação usando a chave secreta.

5. MÉTODO, de acordo com a reivindicação 1, caracterizado pelo fato de que o esquema de compartilhamento secreto limiar compreende um esquema de compartilhamento secreto de Shamir.

6. MÉTODO IMPLEMENTADO POR COMPUTADOR DE UM NÓ DE CONSENSO DE UMA REDE DE PROTOCOLO DE CONFIANÇA (312, 520), o método caracterizado pelo fato de que compreende:

receber um conteúdo de uma transação confidencial (535) de um

nó cliente (302, 530, 304, 540, 306, 308), por um nó de consenso de uma rede de protocolo de confiança (312, 520), em que o conteúdo da transação confidencial (535) compreende:

um ou mais valores de comprometimento da transação confidencial (535) gerada pelo nó cliente (302, 530, 304, 540, 306, 308), através da aplicação de um esquema de comprometimento criptográfico aos dados de transação da transação confidencial (535); e

informação de transação criptografada gerada através da criptografia dos dados de transação usando uma chave secreta do nó cliente (302, 530, 304, 540, 306, 308), em que uma chave secreta é obtida pelo nó cliente (302, 530, 304, 540, 306, 308) de acordo com um esquema de compartilhamento secreto limiar com uma pluralidade de nós clientes (302, 530, 304, 540, 306, 308); e uma ou mais provas de conhecimento zero dos dados de transação;

verificar, através do nó de consenso da rede de protocolo de confiança (312, 520), que a transação confidencial (535) é válida com base no conteúdo da transação confidencial (535); e

armazenar, através do nó de consenso da rede de protocolo de confiança (312, 520), as informações de transação criptografadas em um protocolo de confiança da rede de protocolo de confiança (312, 520).

7. MÉTODO, de acordo com a reivindicação 6, caracterizado pelo fato de que os dados de transação da transação confidencial (535) compreendem um ou mais de um saldo de conta do nó cliente (302, 530, 304, 540, 306, 308) antes da transação confidencial (535), ou um valor de transação da transação confidencial (535).

8. MÉTODO, de acordo com a reivindicação 6, caracterizado pelo fato de que a uma ou mais provas de conhecimento zero dos dados de transação compreende um ou mais intervalos de prova de conhecimento zero

de que os valores dos dados de transação estão dentro dos respectivos intervalos.

9. MÉTODO, de acordo com a reivindicação 6, caracterizado pelo fato de que verificar se a transação confidencial (535) é válida com base no conteúdo da transação confidencial (535) compreende:

determinar que o um ou mais valores de comprometimento estejam corretos com base no esquema de comprometimento; e

verificar as uma ou mais provas de conhecimento zero dos dados de transação.

10. MÉTODO, de acordo com a reivindicação 9, caracterizado pelo fato de que a verificação das uma ou mais provas de conhecimento zero dos dados de transação compreende:

determinar que um saldo de conta do nó cliente (302, 530, 304, 540, 306, 308) antes da transação confidencial (535) é maior que zero; e

determinar que um valor de transação da transação confidencial (535) é menor ou igual a um saldo de conta do nó cliente (302, 530, 304, 540, 306, 308) antes da transação confidencial (535).

11. MÉTODO, de acordo com a reivindicação 6, caracterizado pelo fato de que o esquema de comprometimento criptográfico é homomórfico, e o método compreende ainda a atualização de um saldo de conta do nó cliente (302, 530, 304, 540, 306, 308) após a transação confidencial (535) com base no homomorfismo do esquema de comprometimento.

12. MÉTODO, de acordo com a reivindicação 6, caracterizado pelo fato de que o esquema de compartilhamento secreto limiar compreende um esquema de compartilhamento secreto de Shamir.

13. MÉTODO IMPLEMENTADO POR COMPUTADOR PARA RECUPERAR INFORMAÇÕES DE TRANSAÇÕES CRIPTOGRAFADAS EM TRANSAÇÕES CONFIDENCIAIS DE PROTOCOLO DE CONFIANÇA, o

método caracterizado pelo fato de que compreende:

receber, através de um nó cliente (302, 530, 304, 540, 306, 308) em particular de um nó de consenso de uma rede de protocolo de confiança (312, 520), informações de transação criptografadas de uma transação confidencial (535) do nó cliente (302, 530, 304, 540, 306, 308) em particular, em que as informações de transação criptografadas são armazenadas em pelo menos um protocolo de confiança na rede de protocolo de confiança (312, 520), em que o nó cliente (302, 530, 304, 540, 306, 308) em particular não tem acesso a uma chave secreta configurada para descriptografar as informações de transação criptografada, e em que o nó cliente (302, 530, 304, 540, 306, 308) em particular foi anteriormente emitido a chave secreta;

recuperar, através de um nó cliente (302, 530, 304, 540, 306, 308) em particular, a chave secreta através de pelo menos um número limiar de nó cliente (302, 530, 304, 540, 306, 308)s entre uma pluralidade de nós clientes (302, 530, 304, 540, 306, 308) na rede de protocolo de confiança (312, 520), de acordo com um esquema de compartilhamento secreto limiar, acordado pela pluralidade de nós clientes (302, 530, 304, 540, 306, 308); e

descriptografar, através do nó cliente (302, 530, 304, 540, 306, 308) em particular, dados de transação da transação confidencial (535) do nó cliente (302, 530, 304, 540, 306, 308) em particular através das informações de transação criptografada usando a chave secreta recuperada.

14. MÉTODO, de acordo com a reivindicação 13, caracterizado pelo fato de que o esquema de compartilhamento secreto limiar compreende um esquema de compartilhamento secreto de Shamir.

15. MÉTODO, de acordo com a reivindicação 13, caracterizado pelo fato de que descriptografar dados de transação da transação confidencial (535) do nó cliente (302, 530, 304, 540, 306, 308) em particular, a partir da informação de transação criptografada utilizando a chave secreta compreende

recuperar um valor de transferência da transação confidencial (535) utilizando a chave secreta.

16. MÉTODO, de acordo com a reivindicação 11, caracterizado pelo fato de que descriptografar dados de transação da transação confidencial (535) do nó cliente (302, 530, 304, 540, 306, 308) em particular, a partir da informação de transação criptografada utilizando a chave secreta compreende recuperar tanto o valor de transferência da transação confidencial (535) quanto um número aleatório correspondente ao valor de transferência usando a chave secreta, em que o valor de transferência e o número aleatório são usados em um esquema de comprometimento de Pedersen para ocultar informações de transação da transação confidencial (535) do nó cliente (302, 530, 304, 540, 306, 308) em particular.

17. PRODUTO DE PROGRAMA DE COMPUTADOR, caracterizado pelo fato de que é acoplado a um ou mais processadores e possuindo instruções armazenadas nele que, quando executados por um ou mais processadores, fazem com que o um ou mais processadores executem operações de acordo com o método, conforme definido em qualquer uma das reivindicações 1 a 16.

18. SISTEMA, caracterizado pelo fato de que compreende:

um dispositivo de computação; e

um dispositivo de armazenamento legível por computador acoplado ao dispositivo de computação e possuindo instruções armazenadas nele que, quando executadas pelo dispositivo de computação, fazem com que o dispositivo de computação execute operações de acordo com o método conforme definido em qualquer uma das reivindicações 1 a 16.

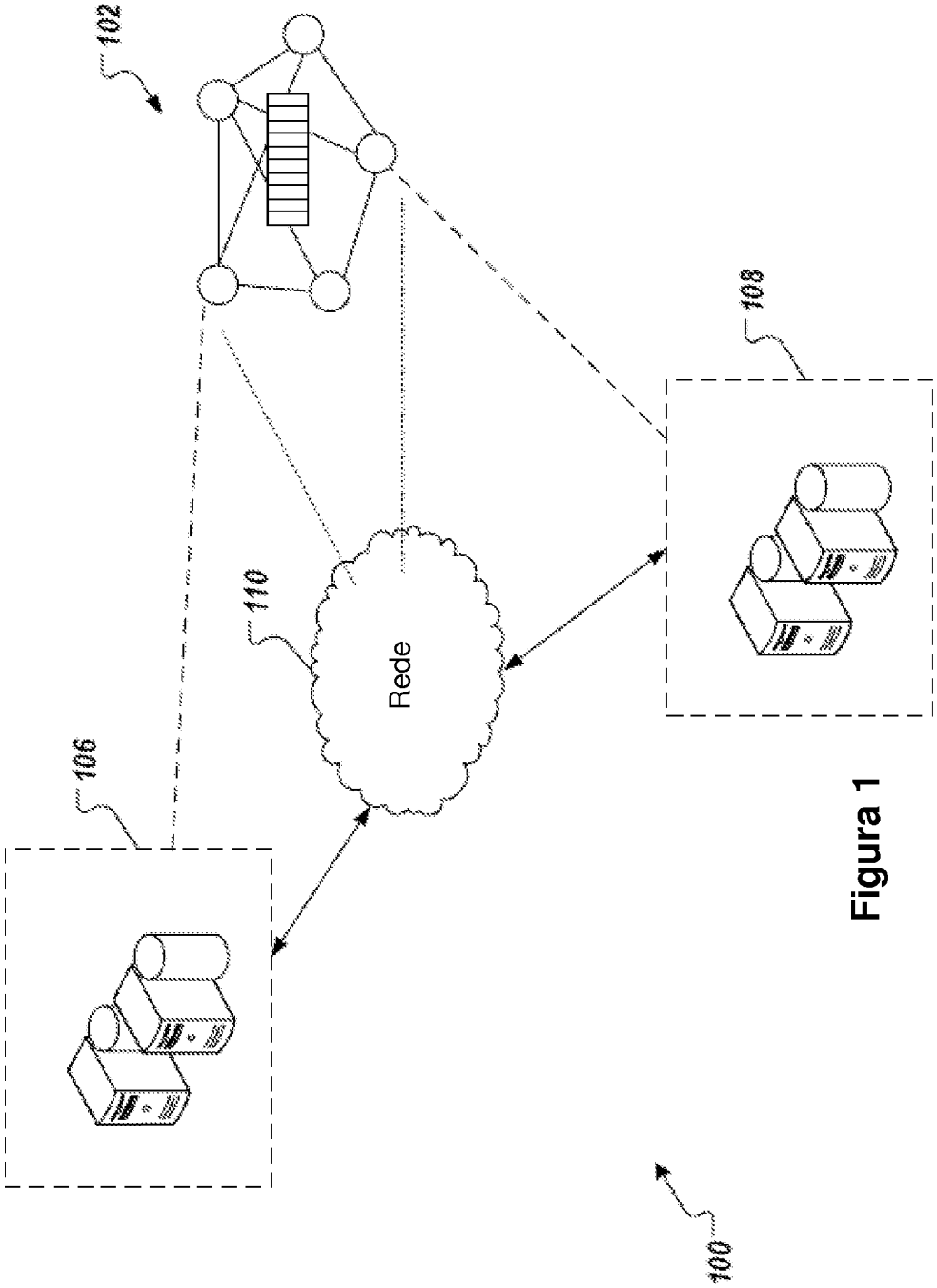

Figura 1

Figura 1

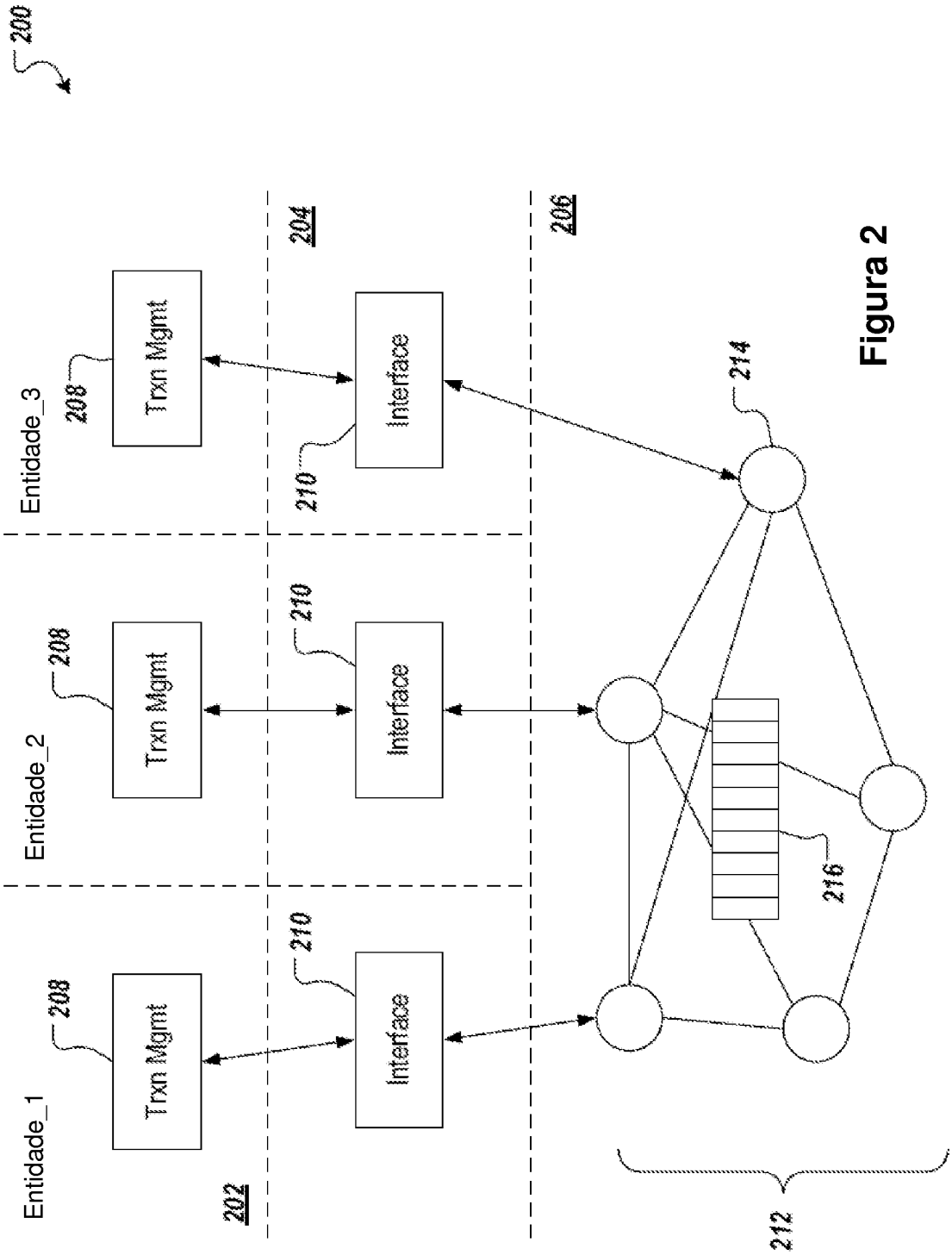
200
Entidade_3
Entidade_2
Entidade_1
208
Trxn Mgmt
210
Interface
202
204
206
212
214
216

Figura 2

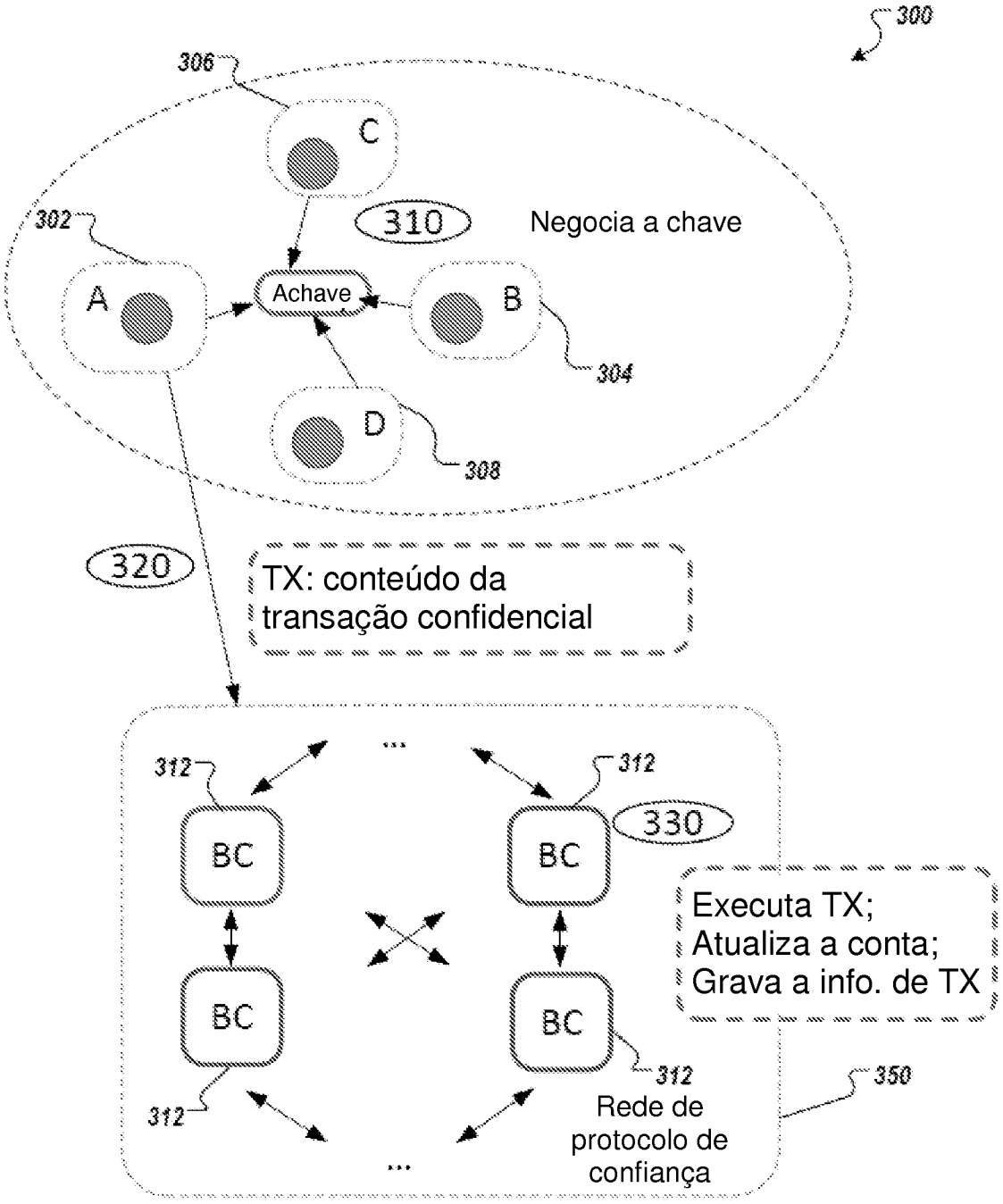
300
306
C
310
Negocia a chave
302
A
Achave
B
304
D
308
320
TX: conteúdo da transação confidencial
312
BC
330
Executa TX;
Atualiza a conta;
Grava a info. de TX
350
Rede de protocolo de confiança

Figura 3

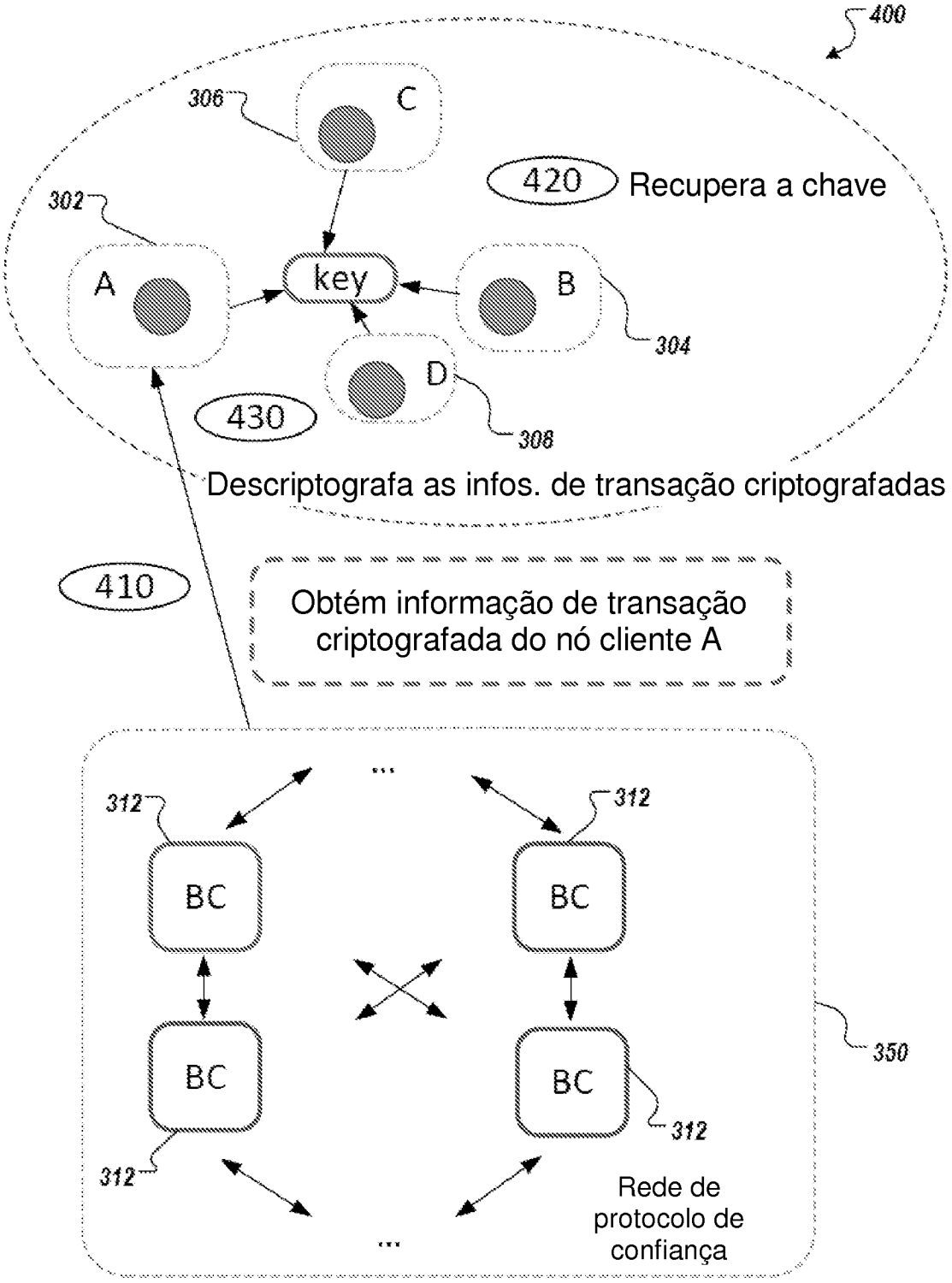
400
306
C
420
Recupera a chave
302
A
key
B
304
D
308
430
Descriptografa as infos. de transação criptografadas
410
Obtém informação de transação criptografada do nó cliente A
312
BC
350
Rede de protocolo de confiança

Figura 4

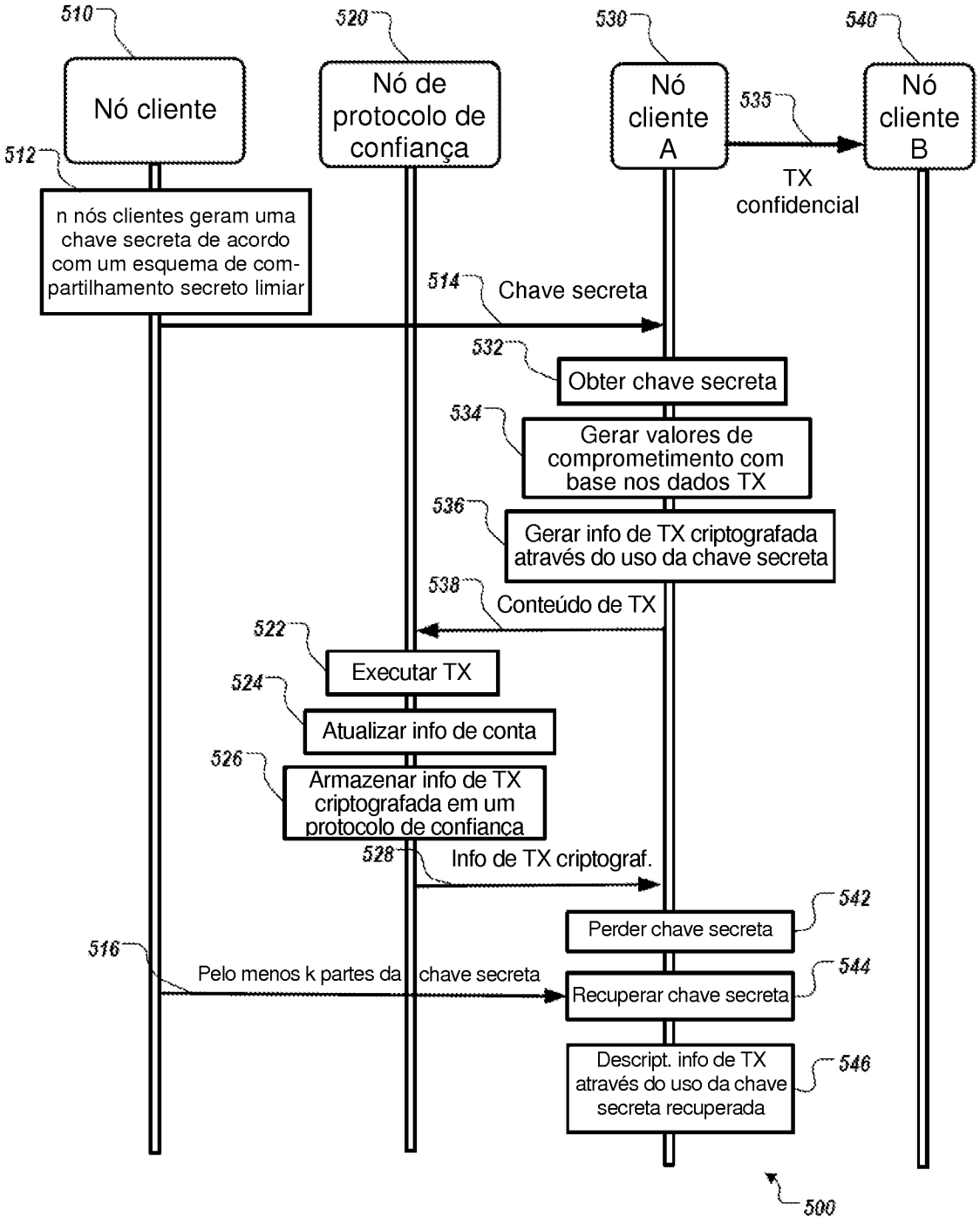
510
Nó cliente
520
Nó de protocolo de confiança
530
Nó cliente A
535
TX confidencial
540
Nó cliente B
512
n nós clientes geram uma chave secreta de acordo com um esquema de com-partilhamento secreto limiar
514
Chave secreta
532
Obter chave secreta
534
Gerar valores de comprometimento com base nos dados TX
536
Gerar info de TX criptografada através do uso da chave secreta
538
Conteúdo de TX
522
Executar TX
524
Atualizar info de conta
526
Armazenar info de TX criptografada em um protocolo de confiança
528
Info de TX criptograf.
542
Perder chave secreta
516
Pelo menos k partes da chave secreta
544
Recuperar chave secreta
546
Descript. info de TX através do uso da chave secreta recuperada
500

Figura 5

RESUMO

"MÉTODO IMPLEMENTADO POR COMPUTADOR DE UM NÓ CLIENTE PARTICIPANDO DE UMA TRANSAÇÃO CONFIDENCIAL DE PROTOCOLO DE CONFIANÇA, MÉTODO IMPLEMENTADO POR COMPUTADOR DE UM NÓ DE CONSENSO DE UMA REDE DE PROTOCOLO DE CONFIANÇA, MÉTODO IMPLEMENTADO POR COMPUTADOR PARA RECUPERAR INFORMAÇÕES DE TRANSAÇÕES CRIPTOGRAFADAS EM TRANSAÇÕES CONFIDENCIAIS DE PROTOCOLO DE CONFIANÇA, PRODUTO DE PROGRAMA DE COMPUTADOR E SISTEMA"

As formas de realização da presente invenção incluem a obtenção de uma chave secreta, através de um nó cliente (302, 530, 304, 540, 306, 308), de acordo com um esquema de compartilhamento secreto limiar acordado por uma pluralidade de nós clientes (302, 530, 304, 540, 306, 308); gerar um ou mais valores de comprometimento de uma transação confidencial (535) do nó cliente (302, 530, 304, 540, 306, 308), através da aplicação de um esquema de comprometimento criptográfico aos dados de transação; gerar informação de transação criptografada da transação confidencial (535), através da criptografia dos dados de transação usando a chave secreta; e transmitir, a um nó de consenso de uma rede de protocolo de confiança (212, 350), um conteúdo da transação confidencial (535) para execução, em que o conteúdo da transação confidencial (535) compreende: o um ou mais valores de comprometimento; as informações de transação criptografadas; e uma ou mais provas de conhecimento zero dos dados de transação.