РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 736 447**(13) **C1**

(51) МПК
G06Q 20/38 (2012.01)
G06Q 40/04 (2012.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06Q 20/3823 *(2020.02);* ***G06Q 20/3825*** *(2020.02);* ***G06Q 20/3829*** *(2020.02);* ***G06Q 20/065*** *(2020.02);* ***G06Q 20/0658*** *(2020.02);* ***G06Q 20/10*** *(2020.02);* ***G06Q 20/223*** *(2020.02);* ***G06Q 20/36*** *(2020.02);* ***G06Q 40/04*** *(2020.02);* ***G06F 16/1824*** *(2020.02);* ***G06F 16/1834*** *(2020.02);* ***H04L 9/0618*** *(2020.02);* ***H04L 9/0643*** *(2020.02);* ***H04L 9/30*** *(2020.02);* ***H04L 9/3218*** *(2020.02)*

(21)(22) Заявка: **2019134841, 31.01.2019**

(24) Дата начала отсчета срока действия патента:
31.01.2019

Дата регистрации:
17.11.2020

Приоритет(ы):
(22) Дата подачи заявки: **31.01.2019**

(45) Опубликовано: **17.11.2020** Бюл. № **32**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **30.10.2019**

(86) Заявка PCT:
CN 2019/074057 (31.01.2019)

(87) Публикация заявки PCT:
WO 2019/072317 (18.04.2019)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр. 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
ЧЖАН, Вэньбинь (CN),
ЛЭЙ, Хао (CN),
ЛИ, Личунь (CN),
ХУАН, Чжанцзе (CN)

(73) Патентообладатель(и):
АЛИБАБА ГРУП ХОЛДИНГ ЛИМИТЕД (KY)

(56) Список документов, цитированных в отчете о поиске: **CN 108335106 A, 27.07.2018. US 2016/0350552 A1, 01.12.2016. US 2018/0189877 A1, 05.07.2018. RU 2673842 C1, 30.11.2018.**

(54) ПЕРЕКРЕСТНАЯ ТОРГОВЛЯ АКТИВАМИ В СЕТЯХ БЛОКЧЕЙНОВ

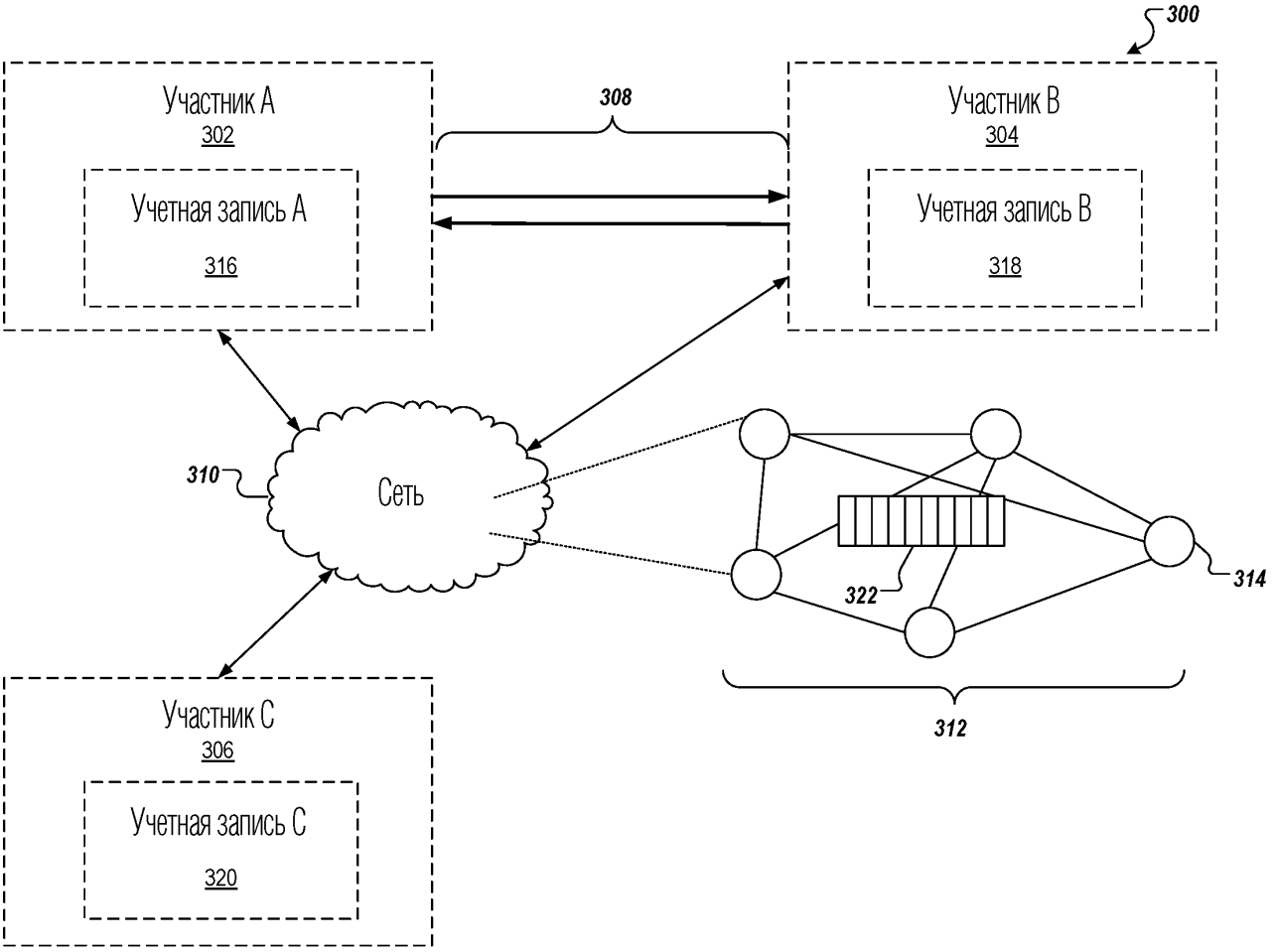
(57) Реферат:

Изобретение относится к области вычислительной техники. Техническим результатом является обеспечение проведения транзакций в сети блокчейнов. Раскрыт компьютерно-реализуемый способ для проведения транзакций в сети блокчейнов, причем способ выполняется одним или несколькими процессорами и содержит: генерирование, первым узлом в сети блокчейнов и с использованием шифрования Boneh–Goh–Nissim (BGN), шифротекстов на основе первого значения и второго значения, причем второе значение определяется на основе гомоморфного умножения первого значения и зашифрованного обменного курса, обеспечиваемого вторым узлом в сети блокчейнов, причем шифротексты и зашифрованный обменный курс находятся на одной и той же эллиптической кривой; передачу, первым узлом второму узлу, первого значения и шифротекстов; прием, первым узлом и от второго узла, первого набора доказательств, содержащего набор данных, которые могут использоваться для верификации обменного курса в процедуре доказательства с нулевым разглашением (ZKP)

RU 2736447 C1

RU 2736447 C1

без раскрытия обменного курса; генерирование первым узлом второго набора доказательств, содержащего набор данных, которые можно использовать для верификации, используя процедуру ZKP, того, что шифротексты зашифрованы открытым ключом BGN первого узла; определение первым узлом транзакции, содержащей первую транзакцию между первым узлом и вторым узлом для перевода первого значения от первого узла второму узлу, и вторую транзакцию между вторым узлом и третьим узлом для перевода второго значения от второго узла к третьему узлу; и передачу первым узлом транзакции по меньшей мере в один консенсусный узел сети блокчейнов для верификации и выполнения транзакции, причем транзакция верифицируется на основе первого набора доказательств и второго набора доказательств, и в ответ на верификацию транзакции выполнение первой транзакции и второй транзакции для уменьшения баланса первого узла на первое значение, увеличения первого баланса второго узла на первое значение, уменьшения второго баланса второго узла на второе значение и увеличения баланса третьего узла на второе значение. 3 н. и 10 з.п. ф-лы, 6 ил.



ФИГ. 3

RU 2736447 C1
RU 2736447 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 736 447**(13) **C1**

(51) Int. Cl.
G06Q 20/38 (2012.01)
G06Q 40/04 (2012.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06Q 20/3823 *(2020.02);* ***G06Q 20/3825*** *(2020.02);* ***G06Q 20/3829*** *(2020.02);* ***G06Q 20/065*** *(2020.02);* ***G06Q 20/0658*** *(2020.02);* ***G06Q 20/10*** *(2020.02);* ***G06Q 20/223*** *(2020.02);* ***G06Q 20/36*** *(2020.02);* ***G06Q 40/04*** *(2020.02);* ***G06F 16/1824*** *(2020.02);* ***G06F 16/1834*** *(2020.02);* ***H04L 9/0618*** *(2020.02);* ***H04L 9/0643*** *(2020.02);* ***H04L 9/30*** *(2020.02);* ***H04L 9/3218*** *(2020.02)*

(21)(22) Application: **2019134841, 31.01.2019**

(24) Effective date for property rights:
31.01.2019

Registration date:
17.11.2020

Priority:
(22) Date of filing: **31.01.2019**

(45) Date of publication: **17.11.2020** Bull. № **32**

(85) Commencement of national phase: **30.10.2019**

(86) PCT application:
CN 2019/074057 (31.01.2019)

(87) PCT publication:
WO 2019/072317 (18.04.2019)

Mail address:
129090, Moskva, ul. B. Spasskaya, 25, str. 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
ZHANG, Wenbin (CN),
LEI, Hao (CN),
LI, Lichun (CN),
HUANG, Zhangjie (CN)

(73) Proprietor(s):
ALIBABA GROUP HOLDING LIMITED (KY)

RU 2736447 C1

(54) ASSET CROSS-TRADE IN NETWORKS OF BLOCKCHAINS

(57) Abstract:

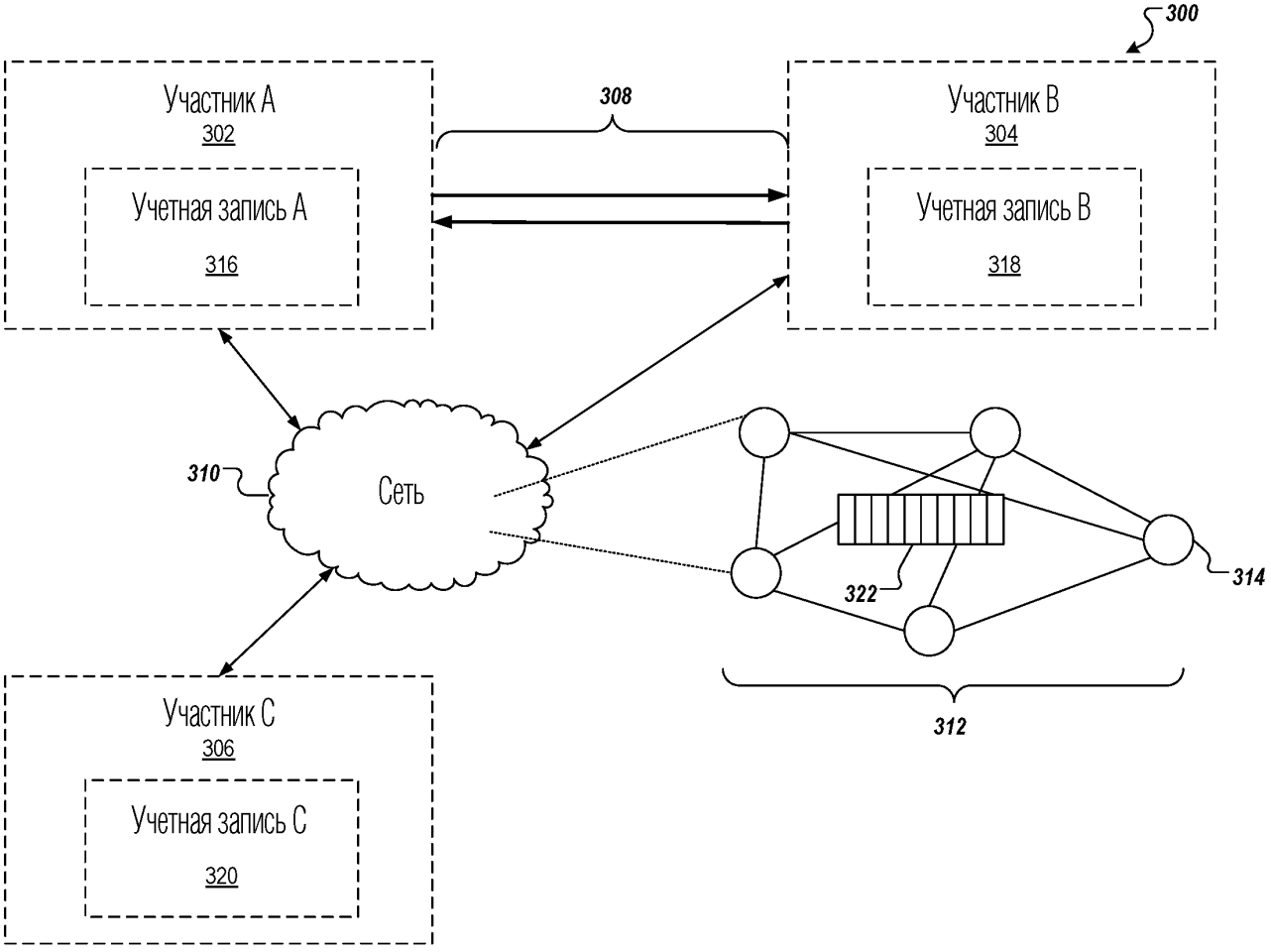
FIELD: computer equipment.

SUBSTANCE: disclosed is a computer-implemented method for conducting transactions in a network of blockchains, wherein the method is carried out by one or more processors and comprises: generating, by the first node in the network of blockchains and using Boneh—Goh—Nissim (BGN) ciphertexts, based on the first value and the second value, wherein second value is determined based on homomorphic multiplication of first value and encrypted exchange rate, provided by the second node in the network of blockchains, wherein ciphertexts and the encrypted exchange rate are on the same elliptic curve; transmitting, by first node to second node, first value and ciphertexts; receiving, by the first node and from the second node, a first set of evidence containing a set of data, which can be used for the exchange rate verification in the zero-disclosure (ZKP) procedure without disclosing the exchange rate; generation by first node of second set of evidence, comprising a set of data which can be used for verification, using the ZKP procedure, that the ciphertexts are encrypted with the public BGN public key of the first node; determination by first transaction node, comprising first transaction between first node and second node to transfer first value from first node to second node, and a second transaction between the second node and the third node to transfer the second value from the second node to

the third node; and transmitting, by first transaction node to, at least, one blockchain network consensus node for verification and execution of transaction, wherein the transaction is verified based on the first set of evidence and the second set of evidence, and in response to transaction verification execution of first transaction and second transaction to reduce first node balance by first value, increase first balance of second node by first value, reducing second balance of second node by second value and increasing balance of third node by second value.

EFFECT: technical result is enabling transactions in a network of blockchains.

13 cl, 6 dwg



ФИГ. 3

RU 2736447 C1

RU 2736447 C1

Уровень техники

[0001] Системы распределенного реестра (DLS), которые также могут называться консенсусными сетями и/или сетями блокчейнов, позволяют участвующим объектам безопасно и постоянно хранить данные. DLS обычно называют сетями блокчейнов, не ссылаясь на какой–либо конкретный вариант использования. Примеры типов сетей блокчейнов могут включать в себя публичные сети блокчейнов, частные сети блокчейнов и консорциальные сети блокчейнов. Публичная сеть блокчейнов открыта для всех объектов, чтобы использовать DLS и участвовать в процессе консенсуса. Для конкретного объекта предоставляется частная сеть блокчейнов, которая централизованно управляет разрешениями на считывание и запись. Консорциальная сеть блокчейнов предоставляется для выбранной группы объектов, которые управляют процессом консенсуса, и включает в себя уровень управления доступом.

[0002] Сети блокчейнов могут использоваться для торговли посредством передачи и обмена цифровыми активами, такими как валюты. Несколько разных типов цифровых активов можно обменивать в сети блокчейнов путем передачи цифровых активов из одного узла сети блокчейнов в другой узел. В некоторых случаях передача цифровых активов в сети блокчейнов предполагает обмен одного типа цифрового актива на второй тип цифрового актива на основе обменного курса.

[0003] Участники в сети блокчейнов, однако, могут желать конфиденциальности в своих транзакциях, так что другие участники, включая консенсусные узлы, не знают деталей транзакции (например, суммы транзакций, обменные курсы). Для обеспечения конфиденциальности могут быть использованы схемы шифрования. Однако некоторые схемы шифрования не поддерживают операции умножения, такие как гомоморфное умножение. Хотя некоторые схемы шифрования поддерживают такие операции умножения, они ограничены только одной операцией умножения. Это ограничивает способность участников в перекрестной транзакции активов, которая включает в себя, например, обменный курс, поддержание конфиденциальности обменного курса.

Сущность изобретения

[0004] Реализации данного описания включают в себя компьютерно реализованные способы для перевода валюты «внутри» сети блокчейнов. Более конкретно, реализации данного описания направлены на перекрестные транзакции активов в сети блокчейнов, используя зашифрованные данные транзакций и зашифрованные обменные курсы.

[0005] В некоторых реализациях действия включают в себя генерирование первым узлом в сети блокчейнов и использование шифрования Boneh–Goh–Nissim (BGN), шифротекстов на основе первого значения и второго значения, причем второе значение определяется на основе первого значения и обменного курса, обеспечиваемого вторым узлом в сети блокчейнов, передачу первым узлом второму узлу первого значения и шифротекстов, прием первым узлом и от второго узла первого набора доказательств, включающего в себя: набор данных, который можно использовать для верификации обменного курса в процедуре доказательства с нулевым разглашением (ZKP) без раскрытия обменного курса, генерирование первым узлом второго набора доказательств, включающего в себя набор данных, которые можно использовать для верификации с использованием процедуры ZKP, что шифротексты шифруются открытым ключом BGN первого узла, определение посредством первого узла транзакции, включающей в себя первую транзакцию между первым узлом и вторым узлом для перевода первого значения из первого узла ко второму узлу и вторую транзакцию между вторым узлом и третьим узлом для перевода второго значения от второго узла к третьему узлу, и передачи первым узлом транзакции по меньшей мере к одному

консенсусному узлу сети блокчейнов для верификации и выполнения транзакции, причем транзакция верифицируется на основе первого набора доказательств и второго набора доказательств, и в ответ на верификацию транзакции выполнение первой транзакции и второй транзакции для уменьшения баланса первого узла на первое значение, увеличения первого баланса второго узла на первое значение, уменьшения второго баланса второго узла на второе значение и увеличения баланса третьего узла на второе значение. Другие реализации включают в себя соответствующие системы, устройства и компьютерные программы, сконфигурированные для выполнения действий способов, закодированных на компьютерных запоминающих устройствах.

[0006] Каждая из этих и других реализаций может необязательно включать в себя одну или несколько из следующих особенностей: первый набор доказательств предоставляется вторым узлом на основе первого значения, пары случайных чисел, предоставленных первым узлом, и шифротекстов; верификация транзакции по меньшей мере одним консенсусным узлом включает в себя верификацию цифровой подписи первого узла и цифровой подписи второго узла; верификация транзакции по меньшей мере одним консенсусным узлом включает в себя верификацию первого доказательства диапазона, предоставленного первым узлом, и второго доказательства диапазона, предоставленного вторым узлом; первое доказательство диапазона включает в себя ZKP для доказательства того, что первое значение больше нуля и что баланс первого узла больше или равен первому значению; второе доказательство диапазона включает в себя ZKP, чтобы доказать, что второй баланс второго узла больше или равен второму значению; транзакция дополнительно включает в себя набор данных, включающий в себя набор шифротекстов, сгенерированных, по меньшей мере, частично, на основе шифрования BGN, причем набор данных используется для верификации транзакции по меньшей мере одним консенсусным узлом; действия дополнительно включают в себя прием первым узлом обменного курса от второго узла через канал под-цепочки сети блокчейнов; по меньшей мере один шифротекст из шифротекстов предоставляется с использованием обязательства Педерсена (Pedersen Commitment); набор данных первого набора доказательств включает в себя первое значение данных и второе значение данных, причем каждое из первого значения данных и второго значения данных определяется на основе параметров, используемых для генерации открытого ключа BGN второго узла; и набор данных второго набора доказательств включает в себя набор шифротекстов и набор значений, причем каждое значение в наборе значений, по меньшей мере, частично основано на хеше набора шифротекстов.

[0007] Данное описание также обеспечивает один или несколько постоянных машиночитаемых носителей данных, подключенных к одному или нескольким процессорам и имеющих на них хранимые инструкции, которые при выполнении одним или несколькими процессорами заставляют один или несколько процессоров выполнять операции в соответствии с реализациями способов, предоставленных здесь.

[0008] Данное описание дополнительно предоставляет систему для реализации способов, предоставленных в данном документе. Система включает в себя один или несколько процессоров и машиночитаемый носитель данных, подключенный к одному или нескольким процессорам, на которых хранятся инструкции, которые при выполнении одним или несколькими процессорами заставляют один или несколько процессоров выполнять операции в соответствии с реализациями способов, предоставленных здесь.

[0009] Понятно, что способы в соответствии с данным описанием могут включать в себя любую комбинацию аспектов и признаков, описанных здесь. То есть способы в соответствии с данным описанием не ограничиваются комбинациями аспектов и

признаков, конкретно описанных в данном документе, но также включают в себя любую комбинацию предоставленных аспектов и признаков.

[0010] Детали одной или нескольких реализаций данного описания изложены на прилагаемых чертежах и в описании ниже. Другие особенности и преимущества данного описания будут очевидны из описания и чертежей, а также из формулы изобретения.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0011] Фиг. 1 изображает пример среды, которая может использоваться для выполнения реализаций данного описания.

[0012] Фиг. 2 изображает пример концептуальной архитектуры в соответствии с реализациями данного описания.

[0013] Фиг. 3 изображает пример платформы для перекрестной торговли активами в соответствии с реализациями данного описания.

[0014] Фиг.4 изображает пример сигнальной схемы для выполнения перекрестной транзакции активов в соответствии с реализациями данного описания.

[0015] Фиг. 5 изображает пример процесса, который может быть выполнен в соответствии с реализациями данного описания.

[0016] Фиг. 6 изображает примеры модулей устройства в соответствии с реализациями данного описания.

[0017] Одинаковые условные обозначения на разных чертежах обозначают одинаковые элементы.

Подробное описание

[0018] Реализации данного описания включают в себя компьютерно реализованные способы для перевода активов в сети блокчейнов. Более конкретно, реализации данного описания направлены на перекрестную транзакцию активов в сети блокчейнов, используя зашифрованные данные транзакций и зашифрованные обменные курсы.

[0019] Для обеспечения дополнительного контекста для реализаций данного описания и, как было показано выше, систем распределенного регистра (DLS), которые также могут называться консенсусными сетями (например, составленными из равноправных узлов), и сетями блокчейнов, разрешают участвующим объектам безопасно и неизменно проводить транзакции и хранить данные. Хотя термин «блокчейн» (цепочка блоков) обычно ассоциируется с конкретными сетями и/или вариантами использования, здесь используется блокчейн, чтобы в целом ссылаться на DLS без ссылки на какой–либо конкретный вариант использования.

[0020] Блокчейн – это структура данных, в которой транзакции хранятся таким образом, что транзакции являются неизменяемыми. Таким образом, транзакции, записанные на блокчейне, являются надежными и заслуживающими доверия. Блокчейн включает в себя один или несколько блоков. Каждый блок в цепочке связан с предыдущим блоком непосредственно перед ним в цепочке путем включения криптографического хеша предыдущего блока. Каждый блок также включает в себя временную метку, свой собственный криптографический хеш и одну или несколько транзакций. Транзакции, которые уже были верифицированы узлами сети блокчейнов, хешируются и кодируются в дерево Меркла. Дерево Меркла – это структура данных, в которой данные в конечных узлах дерева хешируются, и все хеши в каждой ветви дерева объединяются в корне ветви. Этот процесс продолжается вверх по дереву до корня всего дерева, в котором хранится хеш, представляющий все данные в дереве. Хеш, предназначенный для транзакции, хранящейся в дереве, можно быстро верифицировать, определив, соответствует ли он структуре дерева.

[0021] В то время как блокчейн представляет собой децентрализованную или, по

меньшей мере, частично децентрализованную структуру данных для хранения транзакций, сеть блокчейнов представляет собой сеть вычислительных узлов, которые администрируют, обновляют и поддерживают один или несколько блокчейнов путем широковещательной передачи, верификации и утверждения достоверности транзакций и т.д. Консорциальная сеть блокчейнов является частной среди участвующих объектов. В консорциальной сети блокчейнов процесс консенсуса управляется авторизованным набором узлов, одним или несколькими узлами, которые оперируются соответствующим объектом (например, финансовым учреждением, страховой компанией). Например, консорциум из десяти (10) объектов (например, финансовые учреждения, страховые компании) может оперировать консорциальной сетью блокченов, каждый из которых оперирует по меньшей мере одним узлом в консорциальной сети блокчейнов. Соответственно, консорциальная сеть блокчейнов может рассматриваться как частная сеть по отношению к участвующим объектам. В некоторых примерах каждый объект (узел) должен подписывать каждый блок, чтобы этот блок был достоверным и был добавлен в блокчейн. В некоторых примерах, по меньшей мере, поднабор объектов (узлов) (например, по меньшей мере 7 объектов) должен подписать каждый блок, чтобы этот блок был достоверным и был добавлен в блокчейн.

[0022] Как было указано выше, сеть блокчейнов может быть предоставлена как публичная сеть блокчейнов, частная сеть блокчейнов или консорциальная сеть блокчейнов. Реализации данного описания описаны более подробно здесь со ссылкой на консорциальную сеть блокчейнов. Предполагается, однако, что реализации данного описания могут быть реализованы в любом подходящем типе сети блокчейнов. Хотя методы, описанные в данного описания, указаны как относящиеся к консорциальным сетям блокчейнов, методы также могут использоваться, с изменениями или без них, в других типах сетей блокчейнов, включая публичные сети блокчейнов и частные сети блокчейнов.

[0023] В общем, консорциальная сеть блокчейнов является частной среди участвующих объектов. В консорциальной сети блокчейнов процесс консенсуса управляется авторизованным набором узлов, которые могут упоминаться как консенсусные узлы, причем один или несколько консенсусных узлов оперируется соответствующим объектом (например, финансовым учреждением, страховой компанией). Например, консорциум из десяти (10) объектов (например, финансовые учреждения, страховые компании) может оперировать консорциальной сетью блокченов, каждый из которых управляет по меньшей мере одним узлом в консорциальной сети блокчейнов.

[0024] В некоторых примерах в консорциальной сети блокчейнов глобальный блокчейн предоставляется в виде блокчейна, который реплицируется на все узлы. То есть все консенсусные узлы находятся в идеальном состоянии по отношению к глобальному блокчейну. Для достижения консенсуса (например, соглашения о добавлении блока в блокчейн) в консорциальной сети блокчейнов реализован протокол консенсуса. Примеры протоколов консенсуса включают в себя, без ограничения, практическую византийскую отказоустойчивость (PBFT), доказательство работы (POW), доказательство владения (POS) и доказательство полномочий (POA).

[0025] Консорциальные сети блокчейнов могут быть использованы для осуществления переводов и обменов цифровыми активами. В некоторых случаях цифровой актив может представлять собой реальный актив. В некоторых случаях цифровой актив может представлять виртуальный актив. Например, виртуальные активы могут представлять реальную ценность, и их можно использовать для покупки продуктов и/или услуг.

Виртуальные активы предоставляются в качестве альтернативы реальным активам (например, китайский юань, доллар США). Проведение транзакций в консорциальной сети блокчейнов обеспечивает дополнительную безопасность, так как консорциальная сеть блокчейнов верифицирует и неизменно записывает транзакцию. Реализации данного описания описаны более подробно в данном документе со ссылкой на валюты (например, RMB, USD). Однако, предполагается, что реализации могут быть реализованы с любым соответствующим цифровым активом.

[0026] Фиг. 1 изображает пример среды 100, которая может использоваться для выполнения реализаций этой спецификации. В некоторых примерах среда 100 позволяет объектам участвовать в консорциальной сети 102 блокчейнов. Среда 100 включает в себя вычислительные устройства 106, 108 и сеть 110. В некоторых примерах сеть 110 включает в себя локальную сеть (LAN), глобальную сеть (WAN), Интернет или их комбинацию и соединяет веб–сайты, пользовательские устройства (например, вычислительные устройства) и внутренние системы. В некоторых примерах к сети 110 можно получить доступ по проводной и/или беспроводной линии связи.

[0027] В изображенном примере вычислительные системы 106, 108 каждая может включать в себя любую подходящую вычислительную систему, которая обеспечивает возможность участия в качестве узла в консорциальной сети 102 блокчейнов. Примеры вычислительных устройств включают в себя без ограничения сервер, настольный компьютер, ноутбук, планшетное вычислительное устройство и смартфон. В некоторых примерах вычислительные системы 106, 108 размещают на своих ресурсах одну или несколько компьютерно реализованных служб для взаимодействия с консорциальной сетью 102 блокчейнов. Например, вычислительная система 106 может размещать на своих ресурсах компьютерно реализованные услуги первого объекта (например, пользователя A), такие как система администрирования транзакций, которую первый объект использует для администрирования своих транзакций с одним или несколькими другими объектами (например, другими пользователями). Вычислительная система 108 может размещать на своих ресурсах компьютерно реализованные услуги второго объекта (например, пользователя B), такие как система администрирования транзакций, которую второй объект использует для администрирования своих транзакций с одним или несколькими другими объектами (например, другими пользователями). В примере по фиг. 1 консорциальная сеть 102 блокчейнов представлена как сеть равноправных узлов, а вычислительные системы 106, 108 предоставляют узлы первого объекта и второго объекта соответственно, которые участвуют в консорциальной сети 102 блокчейнов.

[0028] Фиг.2 изображает пример концептуальной архитектуры 200 в соответствии с реализациями этой спецификации. Концептуальная архитектура 200 включает в себя уровень 202 объекта, уровень 204 размещенных услуг и уровень 206 сети блокчейнов. В изображенном примере уровень 202 объекта включает в себя трех участников, Участника A, Участника B и Участника C, каждый из которых имеет соответствующую систему 208 администрирования транзакций.

[0029] В изображенном примере уровень 204 размещенных услуг включает в себя интерфейсы 210 для каждой системы 210 администрирования транзакций. В некоторых примерах соответствующая система 208 администрирования транзакций связывается с соответствующим интерфейсом 210 по сети (например, сети 110 по фиг. 1), используя протокол (например, защищенный протокол передачи гипертекста (HTTPS)). В некоторых примерах каждый интерфейс 210 обеспечивает коммуникационное соединение между соответствующей системой 208 администрирования транзакций и уровнем 206

сети блокчейнов. Более конкретно, интерфейс 210 связывается с сетью 212 блокчейнов уровня 206 сети блокчейнов. В некоторых примерах связь между интерфейсом 210 и уровнем 206 сети блокчейнов осуществляется с использованием удаленных вызовов процедур (RPC). В некоторых примерах интерфейсы 210 «размещают на своих ресурсах» (хостируют) сетевые узлы блокчейна для соответствующих систем 208 администрирования транзакций. Например, интерфейсы 210 предоставляют интерфейс прикладного программирования (API) для доступа к сети 212 блокчейнов.

[0030] Как описано в данном документе, сеть 212 блокчейнов предоставляется как одноранговая сеть, включающая в себя множество узлов 214, которые неизменно записывают информацию в блокчейне 216. Хотя схематически изображен один блокчейн 216, предоставляется множественные копии блокчейна 216, которые поддерживаются в сети 212 блокчейнов. Например, каждый узел 214 хранит копию блокчейна. В некоторых реализациях блокчейн 216 хранит информацию, связанную с транзакциями, которые выполняются между двумя или более объектами, участвующими в консорциальной сети блокчейнов.

[0031] Блокчейн (например, блокчейн 216 на фиг. 2) состоит из цепочки блоков, каждый блок хранит данные. Примерные данные включают в себя данные транзакции, представляющие транзакцию между двумя или более участниками. Хотя здесь используются транзакции в качестве неограничивающего примера, предполагается, что любые подходящие данные могут быть сохранены в блокчейне (например, документы, изображения, видео, аудио). Примеры транзакций могут включать в себя, без ограничений, обмены чем–то ценным (например, активами, продуктами, услугами, валютой). Данные транзакции всегда хранятся в блокчейне. То есть данные транзакции не могут быть изменены.

[0032] Перед сохранением в блоке данные транзакции хешируются. Хеширование – это процесс преобразования данных транзакции (предоставляемых в виде строковых данных) в хеш–значение фиксированной длины (также предоставляемое в виде строковых данных). Невозможно обратно преобразовать хеш–значение для получения данных транзакции. Хеширование гарантирует, что даже небольшое изменение данных транзакции приведет к совершенно другому хеш-значению. Дополнительно, как отмечено выше, значение хеш–значения имеет фиксированную длину. То есть независимо от размера данных транзакции длина хеш-значения является фиксированной. Хеширование включает в себя обработку данных транзакции через хеш–функцию для генерации хеш–значения. Пример хеш–функции включает в себя, без ограничения, алгоритм безопасного хеширования (SHA)–256, который выводит 256–битные хеш-значения.

[0033] Данные транзакций множественных транзакций хешируются и сохраняются в блоке. Например, предоставляются значения хеш–значения двух транзакций, и они сами хешируются для предоставления другого хеша. Этот процесс повторяется до тех пор, пока для всех транзакций, которые будут сохранены в блоке, не будет предоставлено одно хеш–значение. Это хеш-значение называется корневым хешем Меркла и хранится в заголовке блока. Изменение в любой из транзакций приведет к изменению ее хеш–значения и, в конечном итоге, к изменению корневого хеша Меркла.

[0034] Блоки добавляются в блокчейн по протоколу консенсуса. Множественные узлы в сети блокчейнов участвуют в протоколе консенсуса и выполняют работу, чтобы добавить блок в блокчейн. Такие узлы называются консенсусными узлами. PBFT, представленный выше, используется в качестве неограничивающего примера протокола консенсуса. Консенсусные узлы выполняют протокол консенсуса для добавления

транзакций в блокчейн.

[0035] Более подробно консенсусный узел генерирует заголовок блока, хеширует все транзакции в блоке и комбинирует хеш–значение в парах, чтобы генерировать дополнительные хеш–значения, пока одно хеш–значение не будет предоставлено для всех транзакций в блоке (корневой хеш Меркла). Этот хеш добавляется в заголовок блока. Консенсусный узел также определяет хеш–значение самого последнего блока в блокчейне (то есть последний блок, добавленный в блокчейн). Консенсусный узел также добавляет одноразовое значение и временную метку к заголовку блока.

[0036] В общем, PBFT обеспечивает практическую реплику византийского конечного автомата, которая допускает византийские ошибки (например, неисправные узлы, вредоносные узлы). Это достигается в PBFT, предполагая, что будут возникать сбои (например, предполагая существование отказов независимых узлов и/или манипулированных сообщений, отправляемых консенсусными узлами). В PBFT консенсусные узлы предоставляются в последовательности, которая включает в себя первичный консенсусный узел и резервные консенсусные узлы. Первичный консенсусный узел периодически изменяется. Транзакции добавляются в блокчейн всеми консенсусными узлами в сети блокчейнов, достигая соглашения относительно мирового состояния сети блокчейнов. В этом процессе сообщения передаются между консенсусными узлами, и каждый консенсусный узел доказывает, что сообщение принято от указанного равноправного узла, и верифицирует, что сообщение не было модифицировано во время передачи.

[0037] В PBFT протокол консенсуса предоставляется в множественные фазы, причем все консенсусные узлы начинаются в одном и том же состоянии. Для начала клиент отправляет запрос первичному консенсусному узлу для вызова служебной операции (например, выполнить транзакцию в сети блокчейнов). В ответ на прием запроса первичный консенсусный узел многоадресно передает запрос резервным консенсусным узлам. Резервные консенсусные узлы выполняют запрос, и каждый отправляет ответ клиенту. Клиент ждет, пока не будет принято пороговое количество ответов. В некоторых примерах клиент ждет приема f+1 ответов, где f – максимальное количество ошибочных консенсусных узлов, которые могут быть допущены в сети блокчейнов. Окончательный результат заключается в том, что достаточное количество консенсусных узлов приходят к соглашению о порядке записи, которая должна быть добавлена в блокчейн, и запись либо принимается, либо отклоняется.

[0038] В некоторых сетях блокчейнов криптография реализуется для поддержания конфиденциальности транзакций. Например, если два узла хотят сохранить конфиденциальность транзакции, так что другие узлы в сети блокчейнов не могут различить детали транзакции, узлы могут зашифровать данные транзакции. Пример криптографии включает в себя, без ограничения, симметричное шифрование и асимметричное шифрование. Симметричное шифрование относится к процессу шифрования, который использует один ключ как для шифрования (генерирования шифротекста из открытого текста), так и для расшифровки (генерирования открытого текста из шифротекста). При симметричном шифровании один и тот же ключ доступен множественным узлам, поэтому каждый узел может зашифровать/расшифровать данные транзакции.

[0039] Асимметричное шифрование использует пары ключей, каждая из которых включает в себя закрытый ключ и открытый ключ, причем закрытый ключ известен только соответствующему узлу, а открытый ключ известен любому или всем другим узлам в сети блокчейнов. Узел может использовать открытый ключ другого узла для

шифрования данных, а зашифрованные данные могут быть расшифрованы с использованием закрытого ключа другого узла. Например, и снова ссылаясь на фиг. 2. Участник А может использовать открытый ключ Участника В для шифрования данных и отправлять зашифрованные данные Участнику В. Участник В может использовать свой закрытый ключ для расшифровки зашифрованных данных (шифротекста) и извлечения исходных данных (открытого текст). Сообщения, зашифрованные открытым ключом узла, могут быть расшифрованы только с помощью закрытого ключа этого узла.

[0040] Асимметричное шифрование используется для предоставления цифровых подписей, что позволяет участникам в транзакции подтверждать других участников в транзакции, а также достоверность транзакции. Например, узел может подписать сообщение цифровой подписью, а другой узел может подтвердить, что сообщение было отправлено узлом на основе цифровой подписи Участника А. Цифровые подписи также могут использоваться для гарантии того, что сообщения не будут подделаны при передаче. Например, и снова ссылаясь на фиг. 2. Участник А должен отправить сообщение Участнику В. Участник А генерирует хеш упомянутого сообщения, а затем, используя свой закрытый ключ, шифрует хеш, чтобы предоставить цифровую подпись в качестве зашифрованного хеша. Участник А добавляет цифровую подпись к сообщению и отправляет сообщение с цифровой подписью Участнику В. Участник В расшифровывает цифровую подпись, используя открытый ключ Участника А, и извлекает хеш. Участник В хеширует сообщение и сравнивает хеши. Если хеши совпадают, Участник В может подтвердить, что сообщение действительно было от Участника А и не было подделано.

[0041] Как и в случае с переводами реальных, физических валют, для эффективного перевода цифрового представления валюты иногда требуется, чтобы получатель обменял первый тип валюты на второй тип валюты. Например, первый член консорциальной сети блокчейнов (например, участник А), имеющий только первый тип валюты (например, доллары США ($)), может захотеть перевести валюту второму члену консорциальной сети блокчейнов (например, Участнику С) во втором типе валюты (например, китайский юань). Для того чтобы Участник А мог перевести значение Участнику С, сумма первого типа валюты обменивается на эквивалентное значение второго типа валюты до перевода Участнику С.

[0042] В соответствии с реализациями данного описания и как описано более подробно здесь, обмен типов валют может быть достигнут через третьего члена консорциальной сети блокчейнов (например, Участника В) в качестве посредника. Например, Участник А может перевести сумму первого типа валюты Участнику В, а Участник В может перевести Участнику С сумму второго типа валюты, имеющую эквивалентное значение на основе обменного курса (ER), используемого Участником В. В некоторых примерах Участник В – это финансовое учреждение, которое предоставляет услуги обмена валюты членам консорциальной сети блокчейнов.

[0043] Чтобы обеспечить конфиденциальность сторон, участвующих в обменах валют в сетях блокчейнов, данные транзакций, лежащие в основе обменов, шифруются до верификации и публикации обмена внутри сети блокчейнов. В некоторых примерах данные транзакции включают в себя сумму перевода первой валюты (t_1) и сумму второй валюты (t_2) предоставленную в обмен на первую сумму. Как правило, данные транзакции, предоставляемые в блокчейн для верификации, шифруются с использованием схемы гомоморфного шифрования, такой как шифрование Boneh–Goh–Nissim (BGN). В схемах гомоморфного шифрования два или более элементов зашифрованных данных

могут быть добавлены вместе без ограничения. В отличие от других схем шифрования (например, шифрование с открытым ключом Пайе (PKE)), шифрование BGN обеспечивает гомоморфное умножение по двум шифротекстам (например, умножение зашифрованного β и зашифрованного t_1). Однако элементы данных, зашифрованные с использованием гомоморфного шифрования, ограничены единичным умножением. Это связано с тем, что мультипликативное спаривание двух элементов данных, зашифрованных с использованием гомоморфного шифрования, генерирует зашифрованный продукт, порядок которого отличается от зашифрованных множителей.

[0044] Приведенное ниже уравнение демонстрирует одноразовый характер мультипликативного гомоморфизма, который обычно называют спариванием на эллиптической кривой $\mathcal{G}$:

$$e{:}\mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G}_1$$

где каждый из умножаемых зашифрованных элементов данных находится на другой эллиптической кривой $\mathcal{G}$, чем произведение умножения, которое находится на $\mathcal{G}_1$. Зашифрованные элементы данных, сгенерированные мультипликативным гомоморфизмом, не могут быть дополнительно умножены или разделены из–за этого изменения базовых эллиптических кривых. Кроме того, зашифрованные элементы данных, сгенерированные мультипликативным гомоморфизмом, нельзя сравнивать с элементами данных, сгенерированными прямым гомоморфным шифрованием. Например, первые два зашифрованных элемента данных в приведенном выше уравнении на одной и той же эллиптической кривой $\mathcal{G}$ можно сравнивать друг с другом, но нельзя сравнивать с третьим зашифрованным элементом данных на эллиптической кривой $\mathcal{G}_1$, сгенерированным мультипликативным гомоморфизмом, из–за разницы базовых эллиптических кривых $\mathcal{G}$и $\mathcal{G}_1$.

[0045] В шифровании BGN каждому участнику i, который должен использовать шифрование BGN, предоставляется пара открытого ключа (PK) BGN, закрытого ключа (SK) (например, PK_{BGN_i},SK_{BGN_o}) посредством процесса генерации ключей. Посредством процесса генерации ключей обеспечивается следующее:

$$PK_{BGN_i} = \{N, G, \mathcal{G}_1, e, P, Q\}_i$$

$$SK_{BGN_i} = p$$

где:

$N = pq$

p, qp, q большие простые числа

$\mathcal{G}$ эллиптическая кривая порядка N

$e{:}\mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G}_1$спаривание

$P \in \mathcal{G}$ генератор

$Q = q\alpha P$ (случайный генератор подгруппы для G, порядок которой равен p)

$\alpha < N$

[0046] В контексте данной спецификации в рамках схем гомоморфного шифрования обменные транзакции, включающие публичный обменный курс, могут верифицироваться и записываться консорциальной сетью блокчейнов без раскрытия или публикации переведенной суммы и/или обменных сумм. Например, как сумма первой валюты (t1), переведенная Участником А Участнику В поставщика услуг обмена, так и сумма второй валюты (t2), предоставленной Участником В в обмен на первую сумму, могут быть

зашифрованы с использованием гомоморфного шифрования. В соответствии с этой схемой и зашифрованная t1, и зашифрованная t2 находятся на эллиптической кривой G. Зашифрованная сумма t_1 перевода может быть умножена на публичный обменный курс Участника B для определения суммы второй валюты, которая должна быть предоставлена Участником B в обмен на t1. Поскольку в этом примере обменный курс Участника B является публичным незашифрованным значением, произведение t1 и публичного обменного курса является зашифрованным элементом данных, который является одной и той же эллиптической кривой $\mathcal{G}$, что и t1. Транзакция обмена между Участником A и Участником B может быть верифицирована сетью блокчейнов путем сравнения зашифрованного произведения t1 и публичного обменного курса зашифрованным элементом t2 данных. Если зашифрованное произведение t1, умноженное на публичный обменный курс, равно зашифрованному элементу t2 данных, то транзакция верифицируется и записывается в блокчейн.

[0047] Хотя эта схема верификации предоставляет эффективные средства для верификации транзакций обмена, связанных с публичными обменными курсами, члены сети блокчейнов, которые предоставляют услуги обмена валют, часто конкурируют с другими такими поставщиками. Следовательно, они не хотят, чтобы их обменные курсы были публичными в сети блокчейнов. Следовательно, желательно, чтобы обменный курс, а также данные транзакции были зашифрованы для транзакций обмена, проводимых внутри и верифицируемых сетью блокчейнов.

[0048] Однако при использовании описанной выше верификации ограничение однократного умножения для гомоморфного шифрования создает барьер для верификации транзакций обмена, в которых как данные транзакции, так и обменный курс шифруются с использованием гомоморфного шифрования. Например, сумма первой валюты (t_1), переведенная Участником A Участнику B поставщика услуг обмена, сумма второй валюты (t_2), на которую переведенная сумма первой валюты была обменена Участником B, и обменный курс (β) Участника B каждый может быть зашифрован с использованием гомоморфного шифрования. Согласно этой схеме зашифрованная (t_1), зашифрованная (t_2) и зашифрованный (β) находятся на одной эллиптической кривой $\mathcal{G}$.

[0049] Как обсуждалось выше, всякий раз, когда обменный курс, участвующий в транзакции обмена, является публичным, транзакция обмена может быть верифицирована сетью блокчейнов путем сравнения произведения (t_1) и публичного обменного курса с зашифрованным элементом t_2 данных. Однако, когда обменный курс зашифрован (β), произведение t_1 и зашифрованного обменного курса (β) находится на эллиптической кривой $\mathcal{G}_1$, которая отличается от базовой кривой $\mathcal{G}$ для t_2. На основании этой разницы в порядке, являющемся результатом мультипликативного гомоморфизма, произведение t_1 на зашифрованный обменный курс (β), можно сравнивать с t_2. В результате при современных схемах верификации верификация транзакций обмена, включающих в себя шифрование как данных транзакций, так и обменного курса, не может проводиться в сети блокчейнов.

[0050] Ввиду вышеупомянутого контекста и как описано более подробно в данном документе, реализации данного описания направлены на перекрестную торговлю активами в сети блокчейнов, используя зашифрованные данные транзакции и зашифрованные обменные курсы. Более конкретно, платформа для перекрестной торговли активами в соответствии с данным описанием позволяет проводить транзакции

с частной (зашифрованной) верификацией обменного курса.

[0051] Фиг. 3 изображает пример платформы 300 для перекрестной торговли активами в соответствии с реализациями этой спецификации. В изображенном примере примерная платформа 300 перекрестной торговли активами включает в себя трех участников, Участника А, Участника В и Участника С, ассоциированных с соответствующими устройствами 302, 304, 306. Примерная платформа 300 перекрестной торговли активами также включает в себя канал 308 под-цепочки, сеть 310 и консорциальную сеть 312 блокчейнов.

[0052] В некоторых примерах сеть 310 включает в себя локальную сеть (LAN), глобальную сеть (WAN), Интернет или их комбинацию и соединяет веб–сайты, пользовательские устройства (например, вычислительные устройства) и внутренние системы. В некоторых примерах к сети 110 можно получить доступ по проводной и/или беспроводной линии связи.

[0053] Как описано в данном документе, сеть 312 блокчейнов предоставляется как одноранговая сеть, включающая в себя множество узлов 314, которые неизменно записывают информацию в блокчейне 322. Несмотря на то, что схематически изображен один блокчейн 322, предоставляется несколько копий блокчейна 322, которые поддерживаются в сети 312 блокчейнов. Например, каждый узел 314 хранит копию блокчейна 322. В некоторых реализациях блокчейн 322 хранит информацию, связанную с транзакциями, которые выполняются между двумя или более объектами, участвующими в консорциальной сети 312 блокчейнов. В некоторых примерах устройства 302, 304, 306 являются частью соответствующих узлов 314 в консорциальной сети 312 блокчейнов.

[0054] В некоторых реализациях устройство 302, устройство 304 и устройство 306 включают в себя соответствующие учетные записи, учетную запись А 316, учетную запись В 318 и учетную запись С 320. В некоторых примерах учетная запись А 316, учетная запись В 318 и учетная запись С 320 хранят финансовые активы. В некоторых примерах учетная запись А 316, учетная запись В 318 и учетная запись С 320 хранят суммы одного или нескольких типов валюты.

[0055] В некоторых реализациях канал 308 под-цепочки может использоваться для передачи информации за пределы сети 312 блокчейнов между двумя членами консорциальной сети 312 блокчейнов. В некоторых примерах частная финансовая информация может быть передана от одного члена консорциальной сети 312 блокчейнов другому члену консорциальной сети 312 блокчейнов за пределами сети 312 блокчейнов по каналу 308 под-цепочки. Например, устройство 304 может передавать частный обменный курс (β) на устройство 302 за пределами сети 312 блокчейнов, передавая обменный курс по каналу 308 под-цепочки.

[0056] В некоторых примерах транзакция между двумя или более членами консорциальной сети 312 блокчейнов может быть предоставлена в сеть 312 блокчейнов для верификации и записи. В некоторых примерах транзакция обмена активами (например, валютой) между двумя или более членами консорциальной сети 312 блокчейнов может быть предоставлена в сеть 312 блокчейнов для верификации обмена. В некоторых примерах информация транзакции, предоставленная в сеть 312 блокчейнов, зашифрована. В некоторых примерах информация транзакции, предоставленная в сеть 312 блокчейнов, шифруется с использованием гомоморфного шифрования. В некоторых примерах информация транзакции включает в себя обменный курс, первую сумму для перевода и вторую сумму для перевода. В некоторых примерах вторая сумма, подлежащая переводу, равна произведению первой суммы на обменный курс.

[0057] Фиг.4 изображает пример сигнальной схемы 400 для выполнения перекрестной транзакции активов в соответствии с реализациями данного описания. Сигнальная схема 400 на фиг. 4 включает в себя учетную запись A 402 (например, узел в сети блокчейнов), учетную запись B 404 (например, узел в сети блокчейнов) и консенсусный узел 406 сети блокчейнов. В некоторых примерах учетная запись A 402 и учетная запись B 404 используются для администрирования активов участников сети блокчейнов (например, Участник A и Участник B соответственно). В некоторых примерах учетная запись A 402 и учетная запись B 404 хранят цифровые активы Участника A и Участника B соответственно. В некоторых примерах Участник B является финансовым учреждением.

[0058] Пример перекрестной транзакции активов описан более подробно со ссылкой на фиг. 4. В примере транзакции сумма (t_1) в первой валюте (например, в долларах США) переводится с Учетной записи A на учетную запись другого участника в сети блокчейнов (например, Участника C) в сумме (t_2) во второй валюте (например, юань). Сумма (t_1) переводится с использованием Учетной записи B 404, посредника, который обеспечивает частный обменный курс (β) между первой валютой и второй валютой. Учетная запись A 402 включает в себя сумму баланса (s_A), которая представляет собой баланс значения в первой валюте, доступной для Учетной записи A 402. Учетная запись B 404 включает в себя первую сумму баланса (s_{B_1}), которая является балансом значения в первой валюте, доступной для Учетной записи B 404, и вторую сумму баланса (s_{B_2}), которая является балансом значения во второй валюте, доступной для Учетной записи B 404.

[0059] В примере перекрестной транзакции активов частный обменный курс (β) передается (408) со Учетной записи B 404 на учетную запись A 402. Сообщение, передающее частный обменный курс, может передаваться по сети. В некоторых примерах сообщение, передающее частный обменный курс, передается по каналу под-цепочки (например, канал 308 под-цепочки по фиг.3).

[0060] Учетная запись 402 генерирует (410) два случайных числа (r1, r2). Учетная запись 402 вычисляет (412) сумму (t2) обмена и наборы шифротекстов (X_1,Y_1,Z_1) и (X_2,Y_2,Z_2). В некоторых реализациях (t_2) равна произведению суммы (t_1), подлежащей переводу, и частного обменного курса (β), как показано ниже:

$$t_2 = \beta t_1$$

В некоторых реализациях наборы шифротекстов (X_1,Y_1,Z_1) и (X_2,Y_2,Z_2) определяются на основе схемы обязательств и схемы шифрования. Пример схемы обязательств включает в себя, без ограничения, обязательство Педерсена (PC). Пример схемы шифрования включает в себя, без ограничения, шифрование BGN. Для шифрования BGN каждый участник включает в себя пару открытого ключа (PK) BGN и закрытого ключа (SK). Например, Учетной записи A 402 назначена пара BGN PK–SK (например, PK_{BGN_A},SK_{BGN_A}), Учетной записи B 404 назначена пара BGN PK–SK (например, PK_{BGN_B},SK_{BGN_B}) и Учетной записи C (не показанный на фиг.4) имеет назначенную ей пару BGN PK–SK (например, PK_{BGN_C},SK_{BGN_C}).

[0061] В некоторых реализациях наборы шифротекстов (X_1,Y_1,Z_1) и (X_2,Y_2,Z_2) соответственно определяются как:

$$(X_1,Y_1,Z_1) = (PC(t_1,r_1),BGN_A(t_1,r_1),BGN_B(t_1,r_1))$$

$$(X_2,Y_2,Z_2) = (PC(t_2,r_2),BGN_B(t_2,r_2),BGN_C(t_2,r_2))$$

Обозначение $PC(t, r)$ указывает обязательство Педерсена для t со случайным числом r в качестве слепого множителя. Обозначение BGN_A указывает шифрование BGN с использованием открытого ключа Учетной записи A 402, обозначение BGN_B указывает шифрование BGN с использованием открытого ключа Учетной записи B 404, а обозначение BGN_C указывает шифрование BGN с использованием открытого ключа Учетной записи C. В некоторых примерах Учетная запись A 402 предоставляет шифротекст баланса в виде:

$$(PC(s_A,\bar{r}_A),BGN_A(s_A,\bar{r}_A))$$

где $\bar{r}_A$ случайное число, сгенерированное Учетной записью A 402.

[0062] Поднаборы шифротекстов (X_1,Z_1) и (X_2,Y_2), случайные числа (r_1, r_2) и сумма (t1) отправляются (414) со Учетной записи A 402 на Учетную запись B 404. В некоторых реализациях сообщение от Учетной записи A 402 к Учетной записи B 404 является зашифрованным сообщением (например, с использованием асимметричного шифрования, описанного выше). В некоторых примерах сообщение передается по каналу под-цепочки (например, каналу 308 под-цепочки по фиг.3). В некоторых примерах (зашифрованное) сообщение включает в себя набор $[t_1,r_1,r_2,X_1,Z_1,X_2,Y_2]$ данных.

[0063] Учетная запись B расшифровывает сообщение, чтобы раскрыть данные (например, $[t_1,r_1,r_2,X_1,Z_1,X_2,Y_2]$. Данные шифротекста верифицируются (416) Учетной записью B 404. В некоторых примерах Учетная запись B 404 верифицирует данные шифротекста, проверяя правильность шифротекстов X_1,Z_1,X_2,Y_2 на основе t_1, r_1, r_2, предоставленных Учетной записью A 402. То есть Учетная запись B пересчитывает X_1, Z_1, X_2, Y_2 и определяет, равны ли они тому, что было принято от Учетной записи A 402. Если шифротексты не равны, ошибка может быть отправлена на Учетную запись A, и транзакция заканчивается.

[0064] Если шифротексты верифицированы, Учетная запись B 404 генерирует (418) доказательство диапазона (RP_B). В некоторых реализациях доказательство диапазона (RP_B) является доказательством с нулевым разглашением (ZKP), которое можно использовать для доказательства того, имеет ли Учетная запись B 404 достаточно средств для выполнения транзакции обмена. Например, доказательство диапазона (RP_B) может быть сгенерировано, чтобы доказать следующее:

$$s_{B_2} - t_2 \geq 0$$

В некоторых примерах Учетная запись B 404 предоставляет первый шифротекст баланса и второй шифротекст баланса, соответственно:

$$(PC(s_{B_1},\bar{r}_{B_1}),BGN_B(s_{B_1},\bar{r}_{B_1}))$$

$$(PC(s_{B_2},\bar{r}_{B_2}),BGN_B(s_{B_2},\bar{r}_{B_2}))$$

где $\bar{r}_{B_1}$ и $\bar{r}_{B_2}$ случайные числа, предоставленные Учетной записью B 404. В некоторых примерах Учетная запись B 404 предоставляет шифротекст обмена в виде:

$$(E',E'') = (PC(\beta,\gamma),BGN_B(\beta,\gamma))$$

где γ случайное число, сгенерированное Учетной записью B 404 и совместно используемое с другими Учетными записями (например, предоставленное Учетной записи A 402 с обменным курсом (β)).

[0065] Генерируется набор (EX) доказательств (420), который можно использовать для верификации частного обменного курса (β). В некоторых реализациях набор (EX) доказательств обменного курса предоставляется как:

$$EX = (U, V, t'', \tilde{r}'', \hat{r}'')$$

В некоторых примерах U и V соответственно рассчитываются как:

$$U = e(P_B, P_B)^{t'} e(P_B, Q_B)^{\tilde{r}'} \text{ и } V = e(P_B, P_B)^{t'} e(P_B, Q_B)^{\hat{r}'}$$

где P_B и Q_B указаны в PK_{BGN_A}, а t', $\tilde{r}'$, and $\hat{r}'$ – случайные числа, сгенерированные Учетной записью B 404. В некоторых примерах $t'', \tilde{r}'', \hat{r}''$ соответственно вычисляются как:

$$t'' = t' + yt_2$$

$$\tilde{r}'' = \tilde{r}' + y\tilde{r}$$

$$\hat{r}'' = \hat{r}' + y\hat{r}$$

где $y = Hash(U,V)$ и $\tilde{r}$ и $\hat{r}$ соответственно рассчитываются как:

$$\tilde{r} = \beta t_1 + t_1\gamma + \gamma r_1 q_B \alpha_B$$

$$\hat{r} = 2t_2 + r_2 q_B \alpha_B$$

В некоторых примерах $Hash$ может быть предоставлен в виде любой подходящей функции хеширования, которая публично известна участникам, включая консенсусные узлы, в сети блокчейнов (например, SHA–256).

[0066] В некоторых реализациях Учетная запись B 404 возвращает (422) зашифрованное сообщение обратно Учетной записи A 402, которая включает в себя следующий примерный набор данных:

$$(X_1, Z_1, X_2, Y_2; RP_B, EX; Sig_B)$$

где Sig_B цифровая подпись Учетной записи B 404. В некоторых примерах сообщение передается по каналу под-цепочки (например, каналу 308 под-цепочки по фиг.3).

[0067] Учетная запись A 402 генерирует (424) доказательство диапазона (RP_A), которое служит в качестве ZKP, что транзакция имеет некоторое значение, и что у Учетной записи A 402 достаточно активов для проведения транзакции. Другими словами, доказательство диапазона (RP_A) может использоваться, чтобы доказать, что:

$$t_1 \geq 0 \text{и } s_A - t_1 \geq 0$$

[0068] Учетная запись A 404 генерирует (426) суб–транзакции, включающие в себя первую суб–транзакцию с Учетной записи A 402 на Учетную запись B 404 для суммы (t_1) и вторую суб–транзакцию с Учетной записи B 404 на Учетную запись C для суммы (t_2). В некоторых примерах Учетная запись A генерирует случайные числа (t', r') и предоставляет набор шифротекстов как:

$$(X', Y', Z') = (PC(t', r'), BGN_A(t', r'), BGN_B(t', r'))$$

Учетная запись A предоставляет набор данных (PF) в виде:

$$PF = (X', Y', Z'; t_1', r_1', t_2', r_2')$$

где:

$$t_1' = t' + xt_1 \text{ , } r_1' = r' + xr_2, \; t_2' = t' + xt_2, \text{ и } r_2' = r' + xr_2$$

где:

$$x = Hash(X', Y', Z')$$

[0069] Учетная запись A 402 предоставляет первую и вторую суб-транзакции соответственно как:

$A, B{:}X_1,Y_1,Z_1$

$B, C{:}\ X_2,Y_2,Z_2$

где A является идентификатором Учетной записи A 402, B является идентификатором Учетной записи B 404, а C является идентификатором Учетной записи C (например, идентификаторы предоставляются в качестве соответствующих адресов в сети блокчейнов). Предоставляется транзакция, которая включает в себя первую и вторую суб-транзакции, доказательства диапазона и вспомогательные наборы доказательств. Например, транзакция предоставляется как:

$A, B{:}\ X_1, Y_1, Z_1; B, C{:}\ X_2, Y_2, Z_2; RP_A, PF; RP_B, EX$

Транзакция имеет цифровую подпись (428) Учетной записи A 402 и включает в себя как подпись Учетной записи A 402 (Sig_A) так и подпись Учетной записи B 404 (Sig_B). Учетная запись A 402 предоставляет (430) подписанную транзакцию в консенсусный узел 406. Подписанная транзакция может быть предоставлена как:

$(A, B{:}X_1,Y_1,Z_1;B, C{:}\ X_2,Y_2,Z_2;RPA, PF;RPB, EX; SigA, SigB)$

[0070] Консенсусный узел 406 верифицирует (432) подписи Учетной записи A 402 и Учетной записи B 404. Если подписи не верифицированы, транзакция заканчивается, и сообщение об ошибке может быть предоставлено Учетной записи A 402. Если подписи верифицированы, доказательство диапазона (RP_A) и доказательство диапазона (RP_B) верифицируются (434) консенсусным узлом 406. Поскольку доказательства диапазона являются ZKP, каждое из них может быть доказано как истинное или возвращать ложное без раскрытия данных в виде открытого текста. Если доказательства диапазона не верифицированы, транзакция заканчивается, и на Учетную запись A 402 может быть отправлено сообщение об ошибке. Если доказательства диапазона верифицированы, то определяется, что сумма транзакции больше 0, и что и у Учетной записи 402, и у Учетной записи 404 достаточно активов в соответствующих валютах для проведения транзакций.

[0071] В некоторых реализациях консенсусный узел 406 верифицирует (436) транзакцию, используя доказательство в наборе данных (PF) и набор (EX) доказательств. В некоторых примерах консенсусный узел 406 верифицирует, являются ли следующие отношения истинными:

$$PC\left(t_1^{'},r_1^{'}\right) = X^{'} + xX_1$$

$$BGN_A\left(t_1^{'},r_1^{'}\right) = Y^{'} + xY_1$$

$$BGN_B\left(t_1^{'},r_1^{'}\right) = Z^{'} + xZ_1$$

$$PC\left(t_2^{'},r_2^{'}\right) = X^{'} + xX_2$$

$$BGN_B\left(t_2^{'},r_2^{'}\right) = Y^{'} + xY_2$$

$$BGN_C\left(t_2^{'},r_2^{'}\right) = Z^{'} + xZ_2$$

где $x = Hash(X', Y', Z')$. Если приведенные выше отношения верны, то подтверждается, что шифротекст (шифротекст BGN) зашифрован с помощью соответствующего открытого ключа, и суммы транзакции являются правильными.

[0072] Также верифицируется, что транзакция проводится по опубликованному (хотя и зашифрованному) обменному курсу. Например, консенсусный узел 406 верифицирует

обменный курс, используя доказательство в наборе (EX) данных. В некоторых примерах консенсусный узел 406 вычисляет $y = Hash(U,V)$, и использует y, чтобы верифицировать, истинны ли следующие отношения:

$$e(P_B, P_B)^{t''} e(P_B, Q_B)^{\tilde{r}''} = U * e(E_2, Z_1)^y$$

$$ePB, PBt()^{''} ePB, QBr()^{''} = V * e(BGN_B(1,1), Y_2)^y$$

[0073] Если отношения не истинны, транзакция и/или обменный курс не верифицированы, транзакция заканчивается, и сообщение об ошибке может быть предоставлено Учетной записи A 402. Если отношения не истинны, консенсусный узел 406 записывает (438) транзакцию, записанную в консорциальная сеть блокчейнов, и балансы учетных записей для Учетной записи A 402, Учетной записи B 404 и Учетной записи C обновляются. Например, баланс (s_A) Учетной записи A 402 уменьшается на сумму (t_1), баланс (s_{B_1}) Учетной записи B 404 увеличивается на сумму (t_1), баланс (s_{B_2}) Учетной записи B 404 уменьшается на сумму (t_2), а баланс Учетной записи C увеличивается на сумму (t_2).

[0074] Фиг. 5 изображает пример процесса 500, который может быть выполнен в соответствии с реализациями данного описания. В некоторых реализациях примерный процесс 500 может выполняться с использованием одной или нескольких компьютерно–исполняемых программ, выполняемых с использованием одного или нескольких вычислительных устройств. В некоторых примерах примерный процесс 500 может выполняться узлами консорциальной сети блокчейнов для проведения перекрестных транзакций активов в сети блокчейнов.

[0075] Принят (502) обменный курс. Например, обменный курс принимается первым узлом, связанным с первым участником в сети блокчейнов (например, узлом сети блокчейнов), от второго узла, связанного со вторым участником в сети блокчейнов (например, узлом сети блокчейнов). В некоторых примерах обменный курс принимается по каналу под-цепочки. В некоторых примерах обменный курс является частным обменным курсом второго участника. В некоторых реализациях вторым участником является финансовое учреждение. В некоторых реализациях обменный курс указывает курс, по которому второй участник обменивает первый тип валюты на второй тип валюты. Например, обменный курс может указывать курс, по которому второй участник будет обменивать доллары США на юани.

[0076] Первое случайное число и второе случайное число генерируются первым узлом (504). Первая сумма и вторая сумма зашифрованы в первом наборе шифротекстов и во втором наборе шифротекстов соответственно с использованием первого случайного числа и второго случайного числа соответственно (506). В некоторых примерах первая сумма представляет собой сумму первого типа активов, которая должна быть переведена первым участником участнику для обмена. В некоторых примерах вторая сумма – это сумма второго типа активов, подлежащая обмену на первую сумму. В некоторых примерах вторая сумма равна произведению первой суммы, на обменный курс второго участника.

[0077] В некоторых примерах первый набор шифротекстов включает в себя обязательство случайного числа первой суммы и первого случайного числа и два гомоморфных шифрования первой суммы и первого случайного числа. В некоторых примерах второй набор шифротекстов включает в себя обязательство случайного числа второй суммы и второго случайного числа и два гомоморфных шифрования второй суммы и второго случайного числа. В некоторых примерах первый набор шифротекстов

включает в себя PC первой суммы и первого случайного числа и шифрование BGN первой суммы и первого случайного числа с использованием открытого ключа BGN первого участника и открытого ключа BGN второго участника соответственно. В некоторых примерах второй набор шифротекстов включает в себя PC второй суммы и второго случайного числа, а также шифрование BGN второй суммы и второго случайного числа с использованием открытого ключа BGN второго участника и открытого ключа BGN третьего участника соответственно.

[0078] Первая сумма, первое случайное число, второе случайное число и, по меньшей мере, часть (поднабор) первого набора шифротекстов и, по меньшей мере, часть (поднабор) второго набора шифротекстов передаются из первого узла на второй узел (508). В некоторых реализациях первая сумма, первое случайное число, второе случайное число, по меньшей мере, часть первого набора шифротекстов и, по меньшей мере, часть второго набора шифротекстов передаются через канал под-цепочки.

[0079] Приняты (510) первое доказательство диапазона, набор доказательств обменного курса и первая подпись. В некоторых реализациях первое доказательство диапазона, набор доказательств обменного курса и первая подпись принимаются первым узлом от второго узла по каналу под-цепочки. В некоторых примерах первая цифровая подпись является цифровой подписью второго участника на основе схемы асимметричного шифрования. В некоторых примерах первое доказательство диапазона предоставляет доказательство того, что учетная запись, связанная со вторым участником, имеет достаточные средства того же типа актива, что и вторая сумма, чтобы обменять первую сумму на вторую сумму.

[0080] Генерируются (512) набор данных, второе доказательство диапазона и вторая цифровая подпись. В некоторых примерах набор данных используется в сети блокчейнов для, по меньшей мере, частичного подтверждения подлинности перекрестной транзакции активов. В некоторых примерах вторая цифровая подпись является цифровой подписью первого участника на основе схемы асимметричного шифрования. В некоторых примерах второе доказательство диапазона обеспечивает доказательство того, что на учетной записи, связанной с первым участником, имеется достаточно средств того же типа актива, что и первая сумма, для перевода первой суммы второму участнику, и что первая сумма не является отрицательной.

[0081] Транзакция предоставляется в сеть блокчейнов для верификации (514). В некоторых реализациях транзакция, предоставленная первым узлом в сеть блокчейнов, включает в себя первый набор шифротекстов, второй набор шифротекстов, первое доказательство диапазона, набор данных, второе доказательство диапазона, набор доказательств обменного курса, первая цифровая подпись и вторая цифровая подпись. В некоторых реализациях по меньшей мере один консенсусный узел в сети блокчейнов верифицирует подписи и доказательства диапазона. В некоторых реализациях по меньшей мере один консенсусный узел верифицирует транзакцию без раскрытия данных транзакции (например, первой суммы, второй суммы, обменного курса). В некоторой реализации, в ответ на успешную верификацию транзакции, транзакция выполняется в сети блокчейнов. В некоторых примерах учетные записи первого участника и второго участника обновляются в блокчейне для отражения обмениваемых активов. В некоторых примерах учетная запись третьего участника обновляется для отражения принятия второй суммы.

[0082] Фиг.6 – схема примера модулей устройства 600 в соответствии с реализациями данного описания. Устройство 600 может быть примером реализации узла блокчейна, сконфигурированного для участия в частной перекрестной торговле активами в сети

блокчейнов, где сеть блокчейнов представляет собой консорциальною сеть блокчейнов. Устройство 600 может соответствовать реализациям, описанным выше, и устройство 600 включает в себя следующее:

[0083] Блок 602 генерирования генерирует, используя шифрование BGN, шифротексты на основе первого значения и второго значения, причем второе значение определяется на основе первого значения и обменного курса, обеспечиваемых вторым узлом в сети блокчейнов. Передающий блок 604 передает первое значение и шифротексты второму узлу. Приемный блок 606 принимает первый набор доказательств, включающий в себя набор данных, которые могут использоваться для верифицирования обменного курса в процедуре ZKP без раскрытия обменного курса. Блок 602 генерирования генерирует второй набор доказательств, включающий в себя набор данных, которые можно использовать для верифицирования, используя процедуру ZKP, того, что шифротексты зашифрованы открытым ключом BGN.

[0084] Блок определения 608 транзакции определяет транзакцию, которая включает в себя первую транзакцию между первым узлом и вторым узлом для передачи первого значения от первого узла ко второму узлу, и вторую транзакцию между вторым узлом и третьим узлом для передачи второго значения от второго узла к третьему узлу. Блок 604 передачи передает транзакцию по меньшей мере одному консенсусному узлу сети блокчейнов для верификации и выполнения транзакции. Как описано здесь, транзакция может быть верифицирована на основе первого набора доказательств и второго набора доказательств. В ответ на верификацию транзакции консенсусный узел выполняет первую транзакцию и вторую транзакцию, чтобы уменьшить баланс первого узла на первое значение, увеличить первый баланс второго узла на первое значение, уменьшить второй баланс второго узла на второе значение и увеличить баланс третьего узла на второе значение.

[0085] В необязательной реализации первый набор доказательств предоставляется вторым узлом на основе первого значения, пары случайных чисел, предоставленных первым узлом, и шифротекстов.

[0086] В необязательной реализации верификация транзакции консенсусным узлом включает в себя верификацию цифровой подписи первого узла и цифровой подписи второго узла.

[0087] В необязательной реализации верификация транзакции консенсусным узлом включает в себя верификацию первого доказательства диапазона, предоставленного первым узлом, и второго доказательства диапазона, предоставленного вторым узлом.

[0088] В необязательной реализации первое доказательство диапазона включает в себя ZKP, чтобы доказать, что первое значение больше нуля и что баланс первого узла больше или равен первому значению.

[0089] В необязательной реализации второе доказательство диапазона включает в себя ZKP, чтобы доказать, что второй баланс второго узла больше или равен второму значению.

[0090] В необязательной реализации транзакция дополнительно включает в себя набор данных, включающий в себя набор шифротекстов, сгенерированных, по меньшей мере, частично, на основе шифрования BGN, причем набор данных используется для верификации транзакции по меньшей мере одним консенсусным узлом.

[0091] В необязательной реализации приемный блок 606 принимает обменный курс от второго узла через канал под-цепочки сети блокчейнов.

[0092] В необязательной реализации по меньшей мере один шифротекст из шифротекстов предоставляется с использованием PC.

[0093] В необязательной реализации набор данных первого набора доказательств включает в себя первое значение данных и второе значение данных, причем каждое из первого значения данных и второго значения данных определяется на основе параметров, используемых для генерации открытого ключа BGN второго узла.

[0094] В необязательной реализации набор данных второго набора доказательств включает в себя набор шифротекстов и набор значений, причем каждое значение в наборе значений, по меньшей мере, частично основано на хеше набора шифротекстов.

[0095] Система, устройство, модуль или блок, проиллюстрированные в предыдущих реализациях, могут быть реализованы с использованием компьютерного чипа или объекта или могут быть реализованы с использованием продукта, имеющего некоторую функцию. Типичным устройством реализации является компьютер, и компьютер может представлять собой персональный компьютер, ноутбук, сотовый телефон, телефон с камерой, смартфон, персональный цифровой помощник, медиаплеер, навигационное устройство, устройство приема и отправки электронной почты, игровая приставка, планшетный компьютер, носимое устройство или любая комбинация этих устройств.

[0096] Для процесса реализации особенностей и ролей каждого блока в устройстве могут быть сделаны ссылки на процесс реализации соответствующих этапов в предыдущем способе. Детали опущены здесь для простоты.

[0097] Поскольку реализация устройства в основном соответствует реализации способа, для связанных частей могут быть сделаны ссылки на связанные описания в реализации способа. Ранее описанная реализация устройства является просто примером. Блоки, описанные как отдельные части, могут быть или не быть физически отдельными, а части, отображаемые как блоки, могут быть или не быть физическими единицами, могут быть расположены в одной позиции или могут быть распределены по ряду сетевых блоков. Некоторые или все модули могут быть выбраны на основе фактических требований для достижения целей решений спецификации. Специалист в данной области техники может понять и реализовать реализации этого приложения без творческих усилий.

[0098] Обращаясь снова к фиг. 6, это можно интерпретировать как иллюстрацию внутреннего функционального модуля и структуры частного устройства перекрестной торговли активами. Частное устройство перекрестной торговли активами может быть примером узла блокчейна, сконфигурированного для участия в частной перекрестной торговле активами в сети блокчейнов. По существу, исполнительным органом может быть электронное устройство, и электронное устройство включает в себя следующее: один или несколько процессоров; и память, сконфигурированную для хранения исполняемой инструкции одного или нескольких процессоров.

[0099] Реализации сущности изобретения и действий и операций, описанных в данного описания, могут быть реализованы в цифровых электронных схемах, в материально–воплощенном компьютерном программном обеспечении или встроенном программном обеспечении, в компьютерном оборудовании, включая структуры, раскрытые в данного описания, и их структурные эквиваленты или в комбинациях одного или нескольких из них. Реализации сущности, описанной в данного описания, могут быть реализованы в виде одной или нескольких компьютерных программ, например, одного или нескольких модулей инструкций компьютерной программы, закодированных на носителе компьютерной программы, для выполнения или для управления операцией устройства обработки данных. Например, носитель компьютерной программы может включать в себя один или несколько машиночитаемых носителей данных, на которых закодированы или сохранены инструкции. Носителем

может быть материальный постоянный машиночитаемый носитель, такой как магнитный, магнитооптический или оптический диск, твердотельный накопитель, оперативное запоминающее устройство (ОЗУ), постоянное запоминающее устройство (ПЗУ) или другое виды СМИ. Альтернативно или в дополнение, носитель может быть искусственно сгенерированным распространяемым сигналом, например, сгенерированным машиной электрическим, оптическим или электромагнитным сигналом, который генерируется для кодирования информации для передачи в подходящее приемное устройство для исполнения устройством обработки данных. Компьютерный носитель данных может быть или быть частью машиночитаемого запоминающего устройства, машиночитаемой подложки запоминающего устройства, устройства памяти с произвольным или последовательным доступом или комбинации одного или нескольких из них. Компьютерный носитель данных не является распространяемым сигналом.

[00100] Компьютерная программа, которая также может упоминаться или описываться как программа, программное обеспечение, программное приложение, приложение, модуль, программный модуль, механизм, сценарий или код, может быть написана на любом языке программирования, включая компилируемые или интерпретируемые языки или декларативные или процедурные языки; и он может быть развернут в любой форме, в том числе как отдельная программа или как модуль, компонент, механизм, подпрограмма или другое устройство, подходящее для выполнения в вычислительной среде, причем эта среда может включать в себя один или несколько компьютеров, соединенных данными сети связи в одном или нескольких местах.

[00101] Компьютерная программа может, но не обязательно, соответствовать файлу в файловой системе. Компьютерная программа может храниться в части файла, которая содержит другие программы или данные, например, в одном или нескольких сценариях, хранящихся в документе на языке разметки, в одном файле, выделенном для рассматриваемой программы, или в нескольких скоординированных файлах, например файлах, в которых хранится один или несколько модулей, подпрограмм или частей кода.

[00102] Процессоры для выполнения компьютерной программы включают в себя, например, как микропроцессоры общего и специального назначения, так и любой один или несколько процессоров любого типа цифрового компьютера. Как правило, процессор будет принимать инструкции компьютерной программы для выполнения, а также данные с неизменяемого машиночитаемого носителя, подключенного к процессору.

[00103] Термин «устройство обработки данных» охватывает все виды устройств, устройств и машин для обработки данных, включая, например, программируемый процессор, компьютер или несколько процессоров или компьютеров. Устройство обработки данных может включать в себя логические схемы специального назначения, например FPGA (программируемая пользователем вентильная матрица), ASIC (специализированная интегральная схема) или GPU (графический процессор). Устройство может также включать в себя, помимо аппаратного обеспечения, код, который создает среду выполнения для компьютерных программ, например код, который составляет микропрограммное обеспечение процессора, стек протоколов, систему управления базой данных, операционную систему или комбинацию одного или нескольких из них.

[00104] Процессы и логические потоки, описанные в данного описания, могут выполняться одним или несколькими компьютерами или процессорами, выполняющими

одну или несколько компьютерных программ для выполнения операций, работая с входными данными и генерируя выходные данные. Процессы и логические потоки также могут выполняться с помощью логических схем специального назначения, например FPGA, ASIC или GPU, или с помощью комбинации логических схем специального назначения и одного или нескольких программируемых компьютеров.

[00105] Компьютеры, подходящие для выполнения компьютерной программы, могут быть основаны на общих или специализированных микропроцессорах или на обоих, или на любом другом типе центрального процессора. Как правило, центральный процессор будет принимать инструкции и данные из постоянной памяти или из оперативной памяти или из обеих. Элементы компьютера могут включать в себя центральный процессор для выполнения инструкций и одно или несколько запоминающих устройств для хранения инструкций и данных. Центральный процессор и память могут быть дополнены или включены в логические схемы специального назначения.

[00106] Как правило, компьютер также будет включать в себя или будет оперативно связан для приема данных или передачи данных на одно или несколько устройств хранения. Запоминающие устройства могут быть, например, магнитными, магнитооптическими или оптическими дисками, твердотельными накопителями или любым другим типом постоянных, машиночитаемых носителей. Однако компьютеру не нужно иметь такие устройства. Таким образом, компьютер может быть связан с одним или несколькими запоминающими устройствами, такими как одно или несколько запоминающих устройств, которые являются локальными и/или удаленными. Например, компьютер может включать в себя одно или несколько локальных запоминающих устройств, которые являются неотъемлемыми компонентами компьютера, или компьютер может быть связан с одним или несколькими удаленными запоминающими устройствами, которые находятся в облачной сети. Кроме того, компьютер может быть встроен в другое устройство, например мобильный телефон, персональный цифровой помощник (PDA), мобильный аудио– или видеоплеер, игровую приставку, приемник глобальной системы позиционирования (GPS) или портативное запоминающее устройство, например, флэш–накопитель с универсальной последовательной шиной (USB), и это лишь некоторые из них.

[00107] Компоненты могут быть «подсоединены» друг к другу, будучи коммутативно такими, как электрически или оптически подсоединенные друг к другу, либо напрямую, либо через один или несколько промежуточных компонентов. Компоненты также могут быть «подсоединены» друг к другу, если один из компонентов интегрирован в другой. Например, компонент хранения, который интегрирован в процессор (например, компонент кэша L2), «подсоединен» к процессору.

[00108] Чтобы обеспечить взаимодействие с пользователем, реализации сущности, описанной в этом описании, могут быть реализованы или сконфигурированы для связи с компьютером, имеющим устройство отображения, например монитор ЖК (жидкокристаллический дисплей), для отображения информации для пользователя и устройство ввода, с помощью которого пользователь может обеспечить ввод в компьютер, например клавиатуру и указательное устройство, например мышь, трекбол или панель касания. Другие виды устройств также могут использоваться для обеспечения взаимодействия с пользователем; например, обратная связь, предоставляемая пользователю, может быть любой формой сенсорной обратной связи, например визуальной обратной связью, слуховой обратной связью или тактильной обратной связью; и ввод от пользователя может быть принят в любой форме, включая

акустический, речевой или тактильный ввод. Кроме того, компьютер может взаимодействовать с пользователем, отправляя документы и принимая документы с устройства, которое используется пользователем; например, путем отправки веб–страниц в веб–браузер на устройстве пользователя в ответ на запросы, принятые из веб–браузера, или путем взаимодействия с приложением, запущенным на пользовательском устройстве, например смартфоном или электронным планшетом. Кроме того, компьютер может взаимодействовать с пользователем, отправляя текстовые сообщения или другие формы сообщений на персональное устройство, например смартфон, на котором запущено приложение обмена сообщениями, и принимая ответные сообщения от пользователя в ответ.

[00109] В данной спецификации используется термин «сконфигурированный для» в связи с системами, устройствами и компонентами компьютерной программы. Если система из одного или нескольких компьютеров настроена на выполнение конкретных операций или действий, это означает, что система установила на нее программное обеспечение, встроенное программное обеспечение, аппаратное обеспечение или их комбинацию, которые при работе заставляют систему выполнять операции или действия. Для одной или нескольких компьютерных программ, которые должны быть сконфигурированы для выполнения определенных операций или действий, это означает, что одна или несколько программ включают в себя инструкции, которые при выполнении устройством обработки данных заставляют устройство выполнять операции или действия. Если логические схемы специального назначения должны быть сконфигурированы для выполнения конкретных операций или действий, это означает, что схема имеет электронную логику, которая выполняет операции или действия.

[00110] Хотя данное описание содержит много конкретных деталей реализации, их не следует истолковывать как ограничения объема заявленной заявки, который определяется самими пунктами формулы изобретения, а скорее как описания особенностей, которые могут быть специфическими для конкретных реализаций. Некоторые особенности, которые описаны в данного описания в контексте отдельных реализаций, также могут быть реализованы в комбинации в одной реализации. И наоборот, различные особенности, которые описаны в контексте отдельных реализаций, также могут быть реализованы в нескольких реализациях отдельно или в любой подходящей субкомбинации. Более того, хотя особенности могут быть описаны выше как действующие в некоторых комбинациях и даже первоначально заявлены как таковые, одна или несколько особенностей из заявленной комбинации могут в некоторых случаях быть исключены из комбинации, и формула может быть направлена на субкомбинацию или вариацию субкомбинации.

[00111] Аналогично, хотя операции изображены на чертежах и изложены в формуле изобретения в конкретном порядке, это не следует понимать как требование, чтобы такие операции выполнялись в конкретном показанном порядке или в последовательном порядке, или чтобы выполнялись все проиллюстрированные операции, чтобы достичь желаемых результатов. В некоторых обстоятельствах многозадачность и параллельная обработка могут быть выгодными. Кроме того, разделение различных системных модулей и компонентов в реализациях, описанных выше, не следует понимать как требующее такого разделения во всех реализациях, и следует понимать, что описанные программные компоненты и системы обычно могут быть объединены вместе в одном программном продукте или упакованы в несколько программных продуктов.

[00112] Конкретные реализации предмета изобретения были описаны. Другие реализации находятся в пределах объема следующей формулы изобретения. Например,

действия, изложенные в формуле изобретения, могут выполняться в другом порядке и при этом достигать желаемых результатов. В качестве одного примера, процессы, изображенные на прилагаемых фигурах, не обязательно требуют конкретного показанного порядка или последовательного порядка для достижения желаемых результатов. В некоторых случаях многозадачность и параллельная обработка могут быть полезными.

(57) Формула изобретения

1. Компьютерно-реализуемый способ для проведения транзакций в сети блокчейнов, причем способ выполняется одним или несколькими процессорами и содержит:

генерирование, первым узлом в сети блокчейнов и с использованием шифрования Boneh–Goh–Nissim (BGN), шифротекстов на основе первого значения и второго значения, причем второе значение определяется на основе гомоморфного умножения первого значения и зашифрованного обменного курса, обеспечиваемого вторым узлом в сети блокчейнов, причем шифротексты и зашифрованный обменный курс находятся на одной и той же эллиптической кривой;

передачу, первым узлом второму узлу, первого значения и шифротекстов;

прием, первым узлом и от второго узла, первого набора доказательств, содержащего набор данных, которые могут использоваться для верификации обменного курса в процедуре доказательства с нулевым разглашением (ZKP) без раскрытия обменного курса;

генерирование первым узлом второго набора доказательств, содержащего набор данных, которые можно использовать для верификации, используя процедуру ZKP, того, что шифротексты зашифрованы открытым ключом BGN первого узла;

определение первым узлом транзакции, содержащей первую транзакцию между первым узлом и вторым узлом для перевода первого значения от первого узла второму узлу, и вторую транзакцию между вторым узлом и третьим узлом для перевода второго значения от второго узла к третьему узлу; и

передачу первым узлом транзакции по меньшей мере в один консенсусный узел сети блокчейнов для верификации и выполнения транзакции, причем транзакция верифицируется на основе первого набора доказательств и второго набора доказательств, и в ответ на верификацию транзакции выполнение первой транзакции и второй транзакции для уменьшения баланса первого узла на первое значение, увеличения первого баланса второго узла на первое значение, уменьшения второго баланса второго узла на второе значение и увеличения баланса третьего узла на второе значение.

2. Способ по п. 1, в котором первый набор доказательств предоставляется вторым узлом на основе первого значения, пары случайных чисел, предоставленных первым узлом, и шифротекстов.

3. Способ по п. 1, в котором верификация транзакции по меньшей мере одним консенсусным узлом содержит верификацию цифровой подписи первого узла и цифровой подписи второго узла.

4. Способ по п. 1, в котором верификация транзакции по меньшей мере одним консенсусным узлом содержит верификацию первого доказательства диапазона, предоставленного первым узлом, и второго доказательства диапазона, предоставленного вторым узлом.

5. Способ по п. 4, в котором первое доказательство диапазона содержит ZKP, чтобы доказать, что первое значение больше нуля и что баланс первого узла больше или равен

первому значению.

6. Способ по п. 4, в котором второе доказательство диапазона содержит ZKP для доказательства того, что второй баланс второго узла больше или равен второму значению.

7. Способ по п. 1, в котором транзакция дополнительно содержит набор данных, содержащий набор шифротекстов, сгенерированных с использованием шифрования BGN, причем этот набор данных используется для верификации транзакции по меньшей мере одним консенсусным узлом.

8. Способ по п. 1, дополнительно содержащий этап, на котором принимают первым узлом обменный курс от второго узла по каналу подцепочки сети блокчейнов.

9. Способ по п. 1, в котором по меньшей мере один шифротекст из упомянутых шифротекстов предоставляется с использованием обязательства Педерсена.

10. Способ по п. 1, в котором набор данных первого набора доказательств содержит первое значение данных и второе значение данных, причем каждое из первого значения данных и второго значения данных определяется на основе параметров, используемых для генерации открытого ключа BGN второго узла.

11. Способ по п. 1, в котором набор данных второго набора доказательств содержит набор шифротекстов и набор значений, причем каждое значение в наборе значений основано на хеше набора шифротекстов.

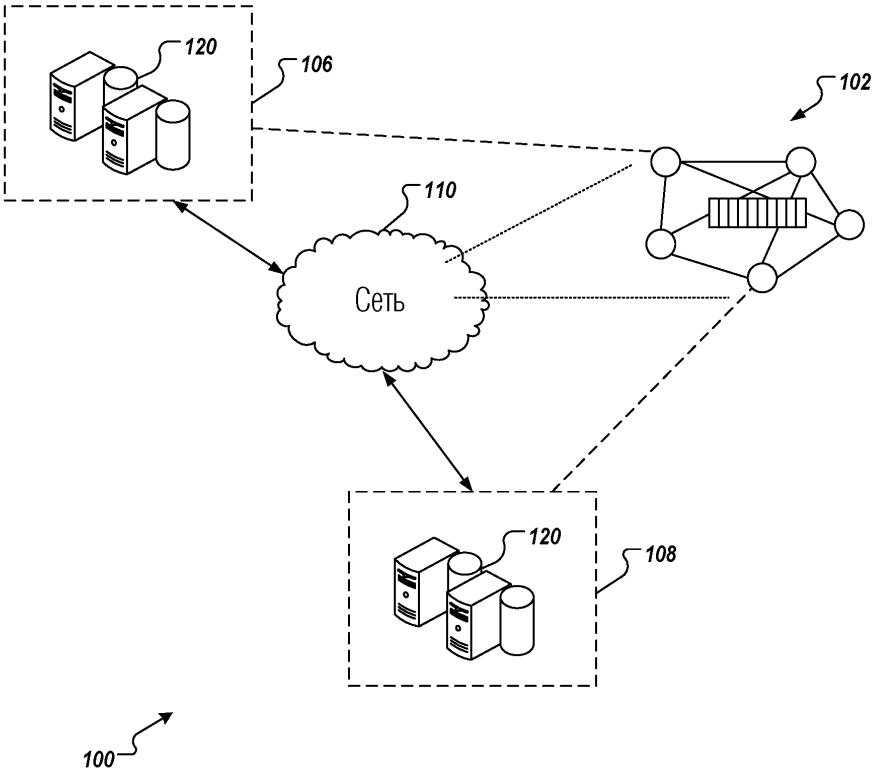
12. Машиночитаемый носитель данных, закодированный с инструкциями для проведения транзакций в сети блокчейнов, причем инструкции выполняются одним или несколькими процессорами и заставляют один или несколько процессоров выполнять способ по любому из предшествующих пунктов.

13. Система для проведения транзакций в сети блокчейнов, содержащая:

один или несколько процессоров; и

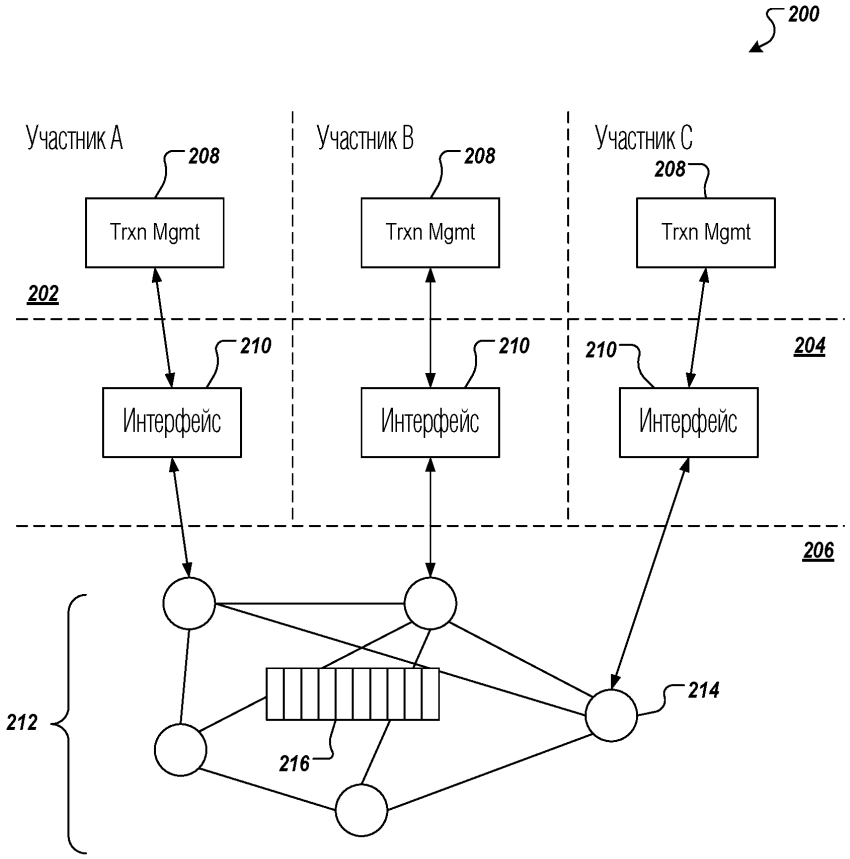
один или несколько машиночитаемых запоминающих устройств, связанных с одним или несколькими процессорами и имеющих хранимые на них инструкции, причем инструкции выполняются одним или несколькими процессорами, чтобы выполнять способ по любому из пп. 1-11.

1



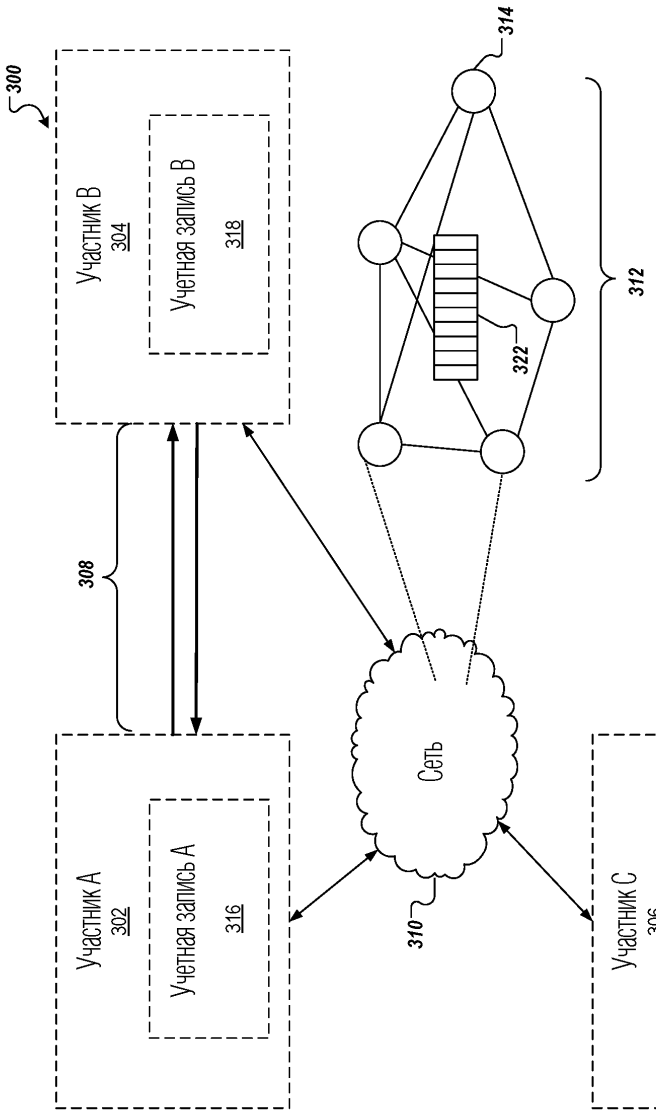
ФИГ. 1

2

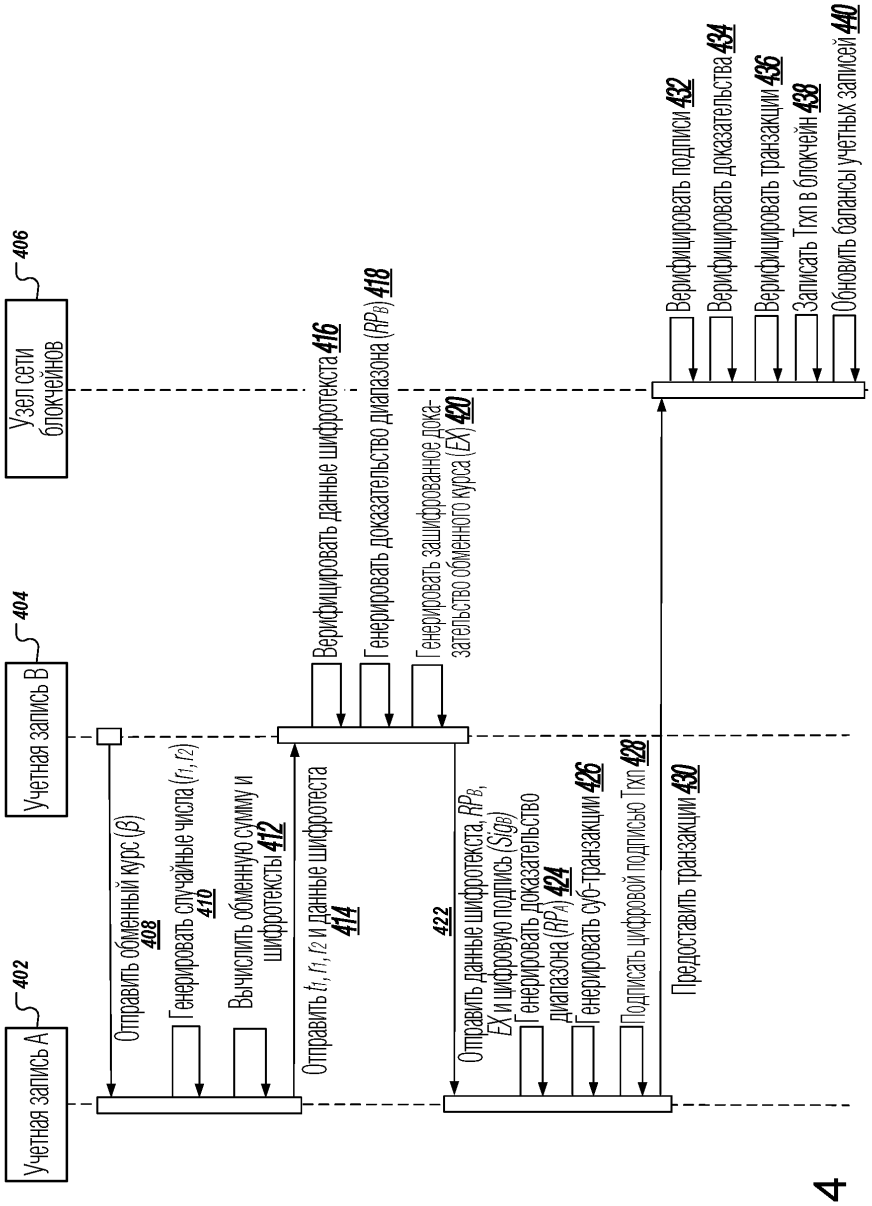

200
Участник A
Участник B
Участник C
208
208
208
Trxn Mgmt
Trxn Mgmt
Trxn Mgmt
202
204
210
210
210
Интерфейс
Интерфейс
Интерфейс
206
212
214
216

ФИГ. 2

3

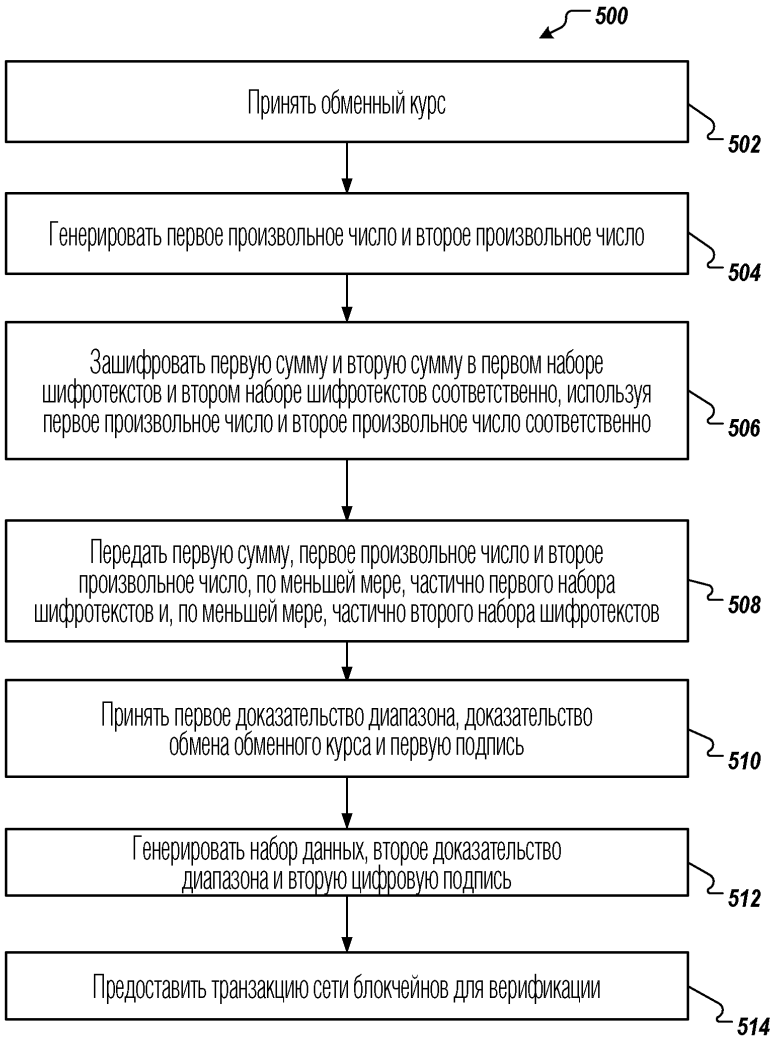

300
Участник B
304
Учетная запись B
318
314
322
312
308
Сеть
310
Участник A
302
Учетная запись A
316
Участник C
306
Учетная запись C
320

ФИГ. 3


Учетная запись A
402
Учетная запись B
404
Узел сети блокчейнов
406
Отправить обменный курс (β) 408
Генерировать случайные числа (r1, r2) 410
Вычислить обменную сумму и шифротексты 412
Отправить t1, r1, r2 и данные шифротеста 414
Верифицировать данные шифротекста 416
Генерировать доказательство диапазона (RPB) 418
Генерировать зашифрованное доказательство обменного курса (EX) 420
Отправить данные шифротекста, RPB, EX и цифровую подпись (SigB) 422
Генерировать доказательство диапазона (RPA) 424
Генерировать суб-транзакции 426
Подписать цифровой подписью Txn 428
Предоставить транзакции 430
Верифицировать подписи 432
Верифицировать доказательства 434
Верифицировать транзакции 436
Записать Txn в блокчейн 438
Обновить балансы учетных записей 440

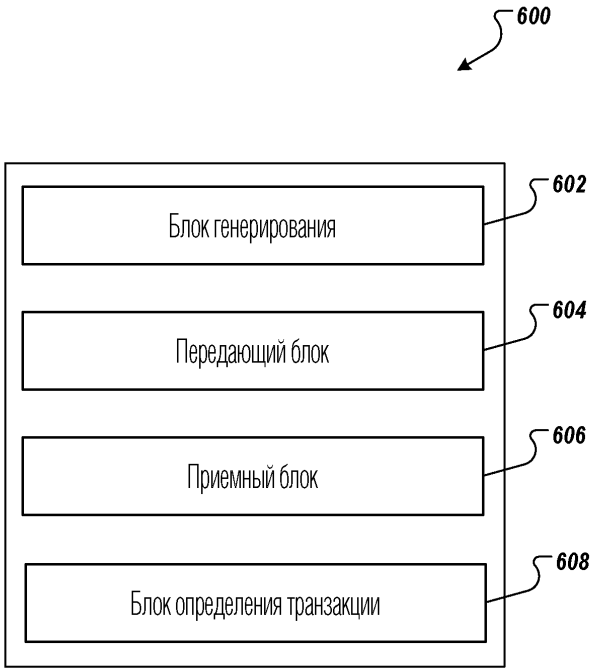
ФИГ. 4

5


500
Принять обменный курс
502
Генерировать первое произвольное число и второе произвольное число
504
Зашифровать первую сумму и вторую сумму в первом наборе шифротекстов и втором наборе шифротекстов соответственно, используя первое произвольное число и второе произвольное число соответственно
506
Передать первую сумму, первое произвольное число и второе произвольное число, по меньшей мере, частично первого набора шифротекстов и, по меньшей мере, частично второго набора шифротекстов
508
Принять первое доказательство диапазона, доказательство обмена обменного курса и первую подпись
510
Генерировать набор данных, второе доказательство диапазона и вторую цифровую подпись
512
Предоставить транзакцию сети блокчейнов для верификации
514

ФИГ. 5

6


600
602
Блок генерирования
604
Передающий блок
606
Приемный блок
608
Блок определения транзакции

ФИГ. 6