РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 733 223**(13) **C1**

(51) МПК
H04L 9/32 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/3247 (2020.05); H04L 9/3239 (2020.05); H04L 9/008 (2020.05)

(21)(22) Заявка: **2019123601, 21.12.2018**

(24) Дата начала отсчета срока действия патента:
21.12.2018

Дата регистрации:
30.09.2020

Приоритет(ы):
(22) Дата подачи заявки: **21.12.2018**

(45) Опубликовано: **30.09.2020** Бюл. № **28**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **26.07.2019**

(86) Заявка PCT:
CN 2018/122573 (21.12.2018)

(87) Публикация заявки PCT:
WO 2019/072302 (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),
МА, Баоли (CN),
МА, Хуаньюй (CN)

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

(56) Список документов, цитированных в отчете о поиске: **US 20160358165 A1, 08.12.2016. US 20180285838 A1, 04.10.2018. CN 107656812 A, 02.02.2018. CN 108764874 A, 06.11.2018. CN 109035029 A, 18.12.2018. CN 109039648 A, 18.12.2018. RU 2674329 C2, 06.12.2018.**

(54) ЗАЩИТА ДАННЫХ ЦЕПОЧЕК БЛОКОВ НА ОСНОВЕ ОБЩЕЙ МОДЕЛИ НА ОСНОВЕ СЧЕТОВ И ГОМОМОРФНОГО ШИФРОВАНИЯ

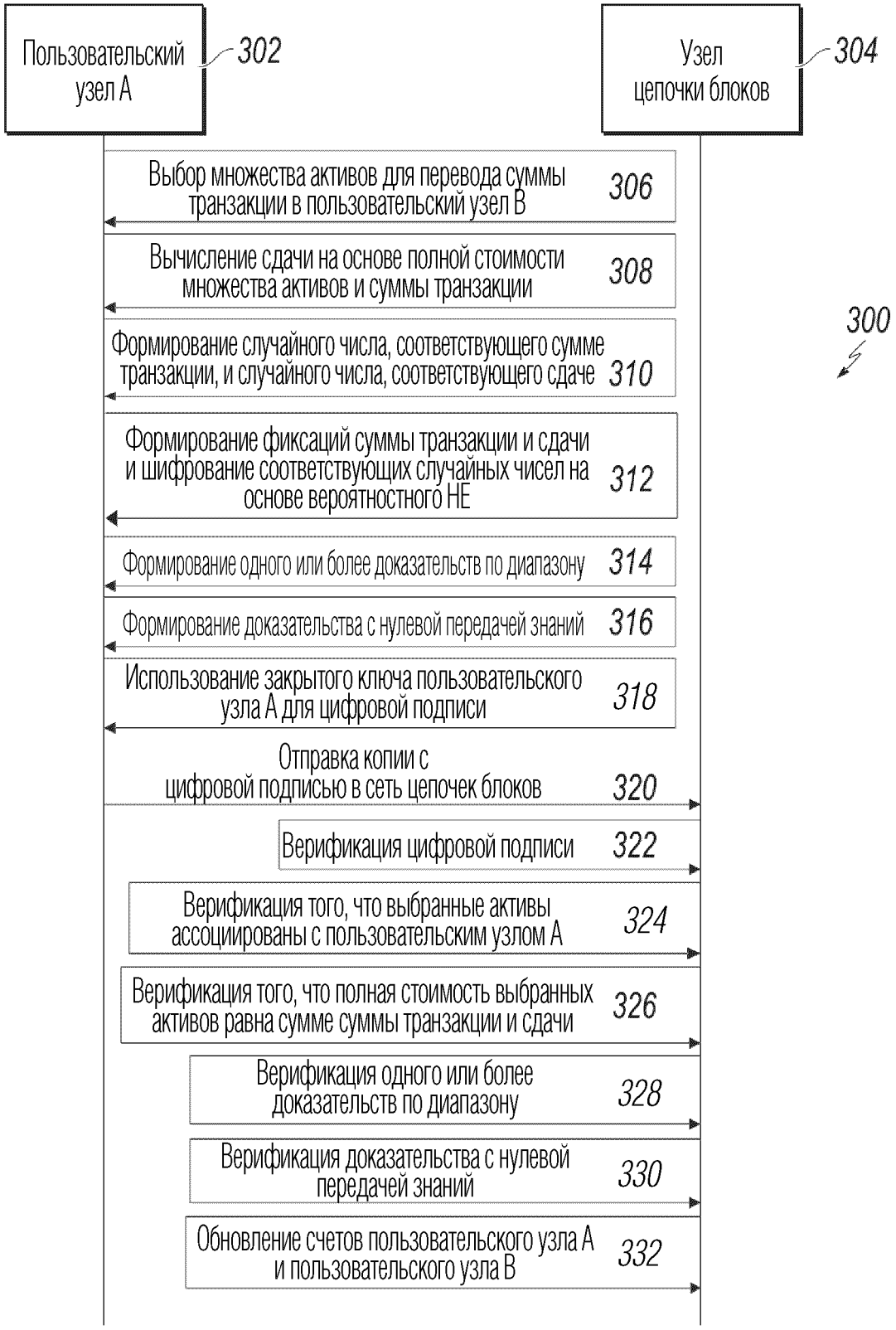
(57) Реферат:

Изобретение относится к области сетей цепочек блоков. Техническим результатом является обеспечение проверки достоверности транзакций без раскрытия конфиденциальной информации. Способ включает в себя прием данных транзакции, ассоциированных с транзакцией, причем данные транзакции содержат: данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, сумму транзакции и третье случайное число, и зашифрованное посредством открытого ключа второго узла на основе линейной детерминированной схемы гомоморфного шифрования (HE), сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе линейной детерминированной HE-схемы, и доказательство с нулевой передачей знаний (ZKP); определение, на основе ZKP, того, является или нет транзакция достоверной, на основе определения того, равно или нет первое случайное число третьему случайному числу, того, равно или нет второе случайное число четвертому случайному числу, и того, равна или нет сумма транзакции, скрытая в первой фиксации, сумме

RU 2733223 C1

RU 2733223 C1

транзакции, зашифрованной посредством открытого ключа второго узла. 3 н. и 8 з.п. ф-лы, 8 ил.



ФИГ. 3

RU 2733223 C1

RU 2733223 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 733 223**(13) **C1**

(51) Int. Cl.
H04L 9/32 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/3247 (2020.05); H04L 9/3239 (2020.05); H04L 9/008 (2020.05)

(21)(22) Application: **2019123601, 21.12.2018**

(24) Effective date for property rights:
21.12.2018

Registration date:
30.09.2020

Priority:
(22) Date of filing: **21.12.2018**

(45) Date of publication: **30.09.2020** Bull. № **28**

(85) Commencement of national phase: **26.07.2019**

(86) PCT application:
CN 2018/122573 (21.12.2018)

(87) PCT publication:
WO 2019/072302 (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),
MA, Baoli (CN),
MA, Huanyu (CN)

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

RU 2733223 C1

(54) PROTECTION OF DATA OF CHAINS OF BLOCKS BASED ON COMMON MODEL BASED ON ACCOUNTS AND HOMOMORPHIC ENCRYPTION

(57) Abstract:

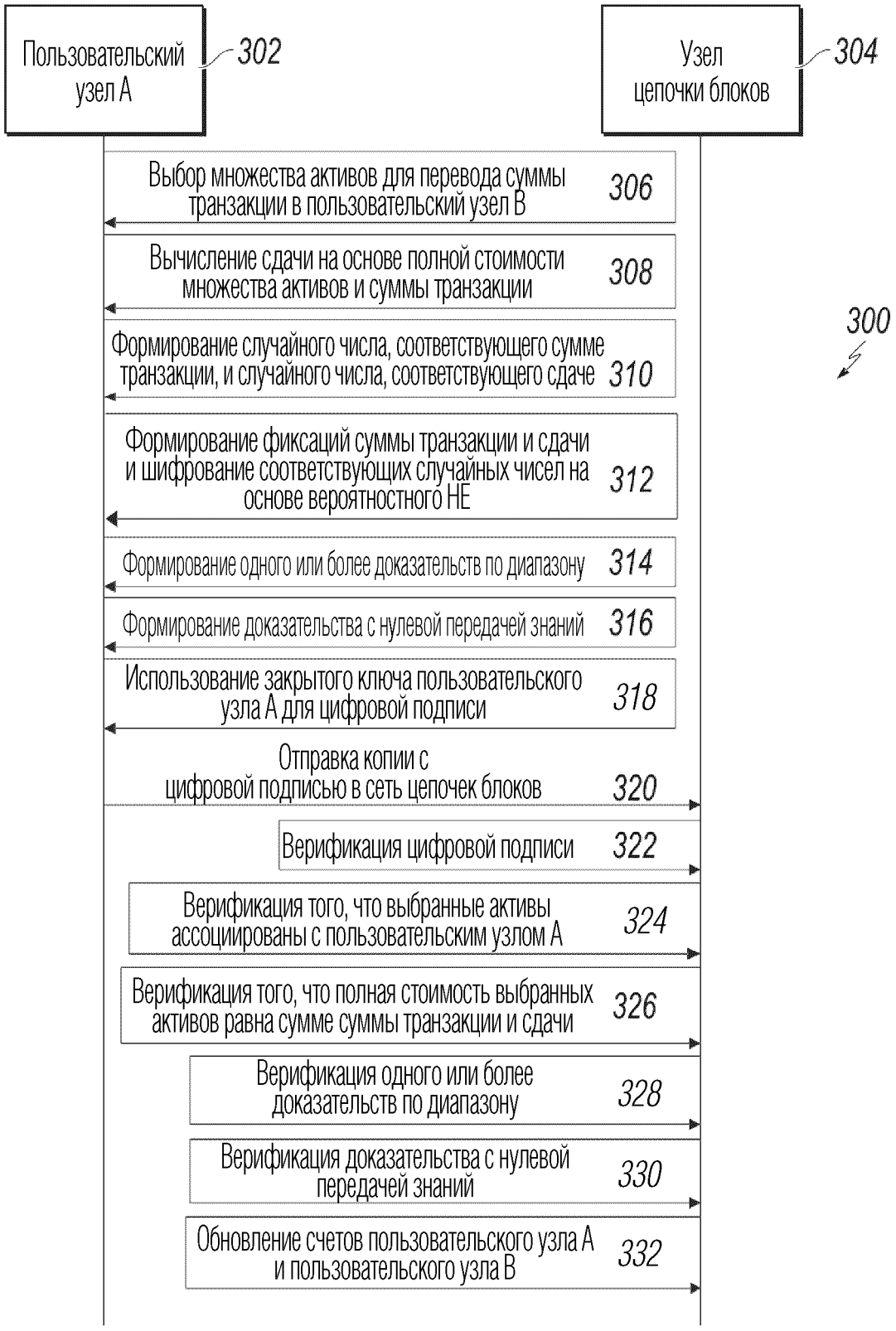
FIELD: network of chains of blocks.

SUBSTANCE: method includes receiving transaction data associated with a transaction, wherein the transaction data comprises: data representing a plurality of assets, a first commit, which hides first random number and transaction amount for transaction, second commit, which hides second random number and surrender, transaction amount and third random number, and encrypted by means of public key of second node based on linear deterministic scheme of homomorphic encryption (HE), surrendering and fourth random number, both of which are encrypted by means of public key of first node based on linear deterministic HE-scheme, and proof with zero transfer of knowledge (ZKP); determining, based on ZKP, whether the transaction is valid, based on determining whether or not the first random number is equal to the third random number, whether or not the second random number is equal to the fourth random number, and whether the transaction sum hidden in the first commit is equal to the sum of the transaction encrypted by the second node public key.

EFFECT: technical result is ensuring verification of transactions without disclosing confidential information.

11 cl, 8 dwg

RU 2733223 C1



ФИГ. 3

RU 2733223 C1

Уровень техники

[0001] Сети цепочек блоков, которые также могут упоминаться как системы цепочек блоков, консенсусные сети, сети на основе системы распределенных реестров или цепочка блоков, позволяют участвующим объектам защищенно и неизменно сохранять данные. Цепочка блоков может описываться как реестр транзакций, и несколько копий цепочки блоков сохраняются в сети цепочек блоков. Примерные типы цепочек блоков могут включать в себя открытые цепочки блоков, консорциальные цепочки блоков и закрытые цепочки блоков. Открытая цепочка блоков является открытой для всех объектов в том, чтобы использовать цепочку блоков и участвовать в консенсусном процессе. Консорциальная цепочка блоков представляет собой цепочку блоков, в которой консенсусный процесс управляется посредством заранее выбранного набора узлов, таких как определенные организации или учреждения. Закрытая цепочка блоков предоставляется для конкретного объекта, который централизованно управляет разрешениями на считывание и запись.

[0002] Цепочки блоков могут использовать различные модели ведения записей для того, чтобы записывать транзакции между пользователями. Примерные модели ведения записей включают в себя модель на основе непотраченного вывода по транзакциям (UTXO) и модель на основе баланса счетов. В UTXO-модели, каждая транзакция тратит вывод из предшествующих транзакций и формирует новые выводы, которые могут тратиться в последующих транзакциях. Непотраченные транзакции пользователя отслеживаются, и баланс, который является доступным для того чтобы тратить, вычисляется как суммарная величина непотраченных транзакций. В модели на основе баланса счетов, баланс счета каждого пользователя отслеживается как глобальное состояние. Для каждой транзакции, баланс счета расходов проверяется, чтобы удостоверяться в том, что он больше или равен сумме транзакции. Это является сравнимым с традиционным банковским делом.

[0003] Цепочка блоков включает в себя последовательность блоков, каждый из которых содержит одну или более транзакций, выполняемых в сети. Каждый блок может быть аналогичным странице реестра, в то время как сама цепочка блоков является полной копией реестра. Отдельные транзакции подтверждаются и добавляются в блок, который добавляется в цепочку блоков. Копии цепочки блоков реплицируются в узлах сети. Таким образом, предусмотрен глобальный консенсус по состоянию цепочки блоков. Дополнительно, цепочка блоков является открытой для наблюдения посредством всех узлов, по меньшей мере, в случае открытых сетей. Чтобы защищать конфиденциальность пользователей цепочек блоков, реализуются технологии шифрования.

[0004] Согласно модели на основе баланса счетов, схемы фиксации могут использоваться для того, чтобы скрывать стоимости, которые фиксируют обе стороны транзакции. Схемы фиксации могут возникать в силу потребности для сторон фиксировать выбор или стоимость и впоследствии передавать эту стоимость другим участвующим сторонам. Например, в интерактивной схеме фиксации Педерсена (PC), первый пользователь может фиксировать на сумму t транзакции посредством отправки стоимости PC(t, r) фиксации, которая формируется на основе случайного значения r. Стоимость фиксации формируется, и второй пользователь может раскрывать сумму t транзакции только посредством получения случайного числа r. Чтобы обеспечивать то, что сумма транзакции является достоверной, доказательство по диапазону может создаваться, чтобы доказывать то, что сумма транзакции превышает или равна нулю и меньше или равна балансу счета.

[0005] В некоторых случаях, несколько транзакций могут проводиться от пользователя. Поскольку доказательство по диапазону ассоциировано с оставшимся балансом счета, несколько транзакций должны верифицироваться последовательно в цепочке блоков. В связи с этим, соответствующие доказательства по диапазону могут быть корректно ассоциированы с оставшимися балансами счета после каждой транзакции. Тем не менее, последовательная верификация нескольких транзакций может быть времязатратной. Модель ведения записей, которая обеспечивает возможность параллельных верификаций транзакций, должна быть преимущественной специально для чувствительных ко времени задач.

Сущность изобретения

[0006] Реализации описания изобретения включают в себя машинореализованные способы для неинтерактивных верификаций с сохранением конфиденциальности транзакций с цепочками блоков. Более конкретно, реализации описания изобретения направлены на машинореализованный способ, допускающий параллельную проверку достоверности нескольких транзакций, ассоциированных со счетом узла цепочки блоков, на основе схем фиксации и гомоморфного шифрования без раскрытия конфиденциальной информации, такой как сумма транзакции, баланс счетов или случайные числа для формирования фиксаций, для других узлов цепочки блоков.

[0007] В некоторых реализациях, действия включают в себя прием данных транзакции, ассоциированных с транзакцией, причем данные транзакции содержат: данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, вычисленную на основе удержания суммы транзакции из полной стоимости множества активов, сумму транзакции и третье случайное число, оба из которых шифруются посредством открытого ключа второго узла на основе линейной детерминированной схемы шифрования (HE), сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе линейной детерминированной HE-схемы, одно или более доказательств по диапазону, доказательство с нулевой передачей знаний (ZKP) и цифровую подпись, сформированную на основе закрытого ключа, соответствующего открытому ключу первого узла; верификацию цифровой подписи на основе открытого ключа первого узла; определение того, что одно или более доказательств по диапазону доказывают то, что сумма транзакции и сдача больше или равны нулю; определение того, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи; и определение, на основе ZKP, того, что транзакция является достоверной, посредством определения того, что первое случайное число равно третьему случайному числу, второе случайное число равно четвертому случайному числу, и сумма транзакции, скрытая в первой фиксации, равна сумме транзакции, зашифрованной посредством открытого ключа второго узла. Другие реализации включают в себя соответствующие системы, оборудование и компьютерные программы, выполненные с возможностью выполнять действия способов, кодированных на компьютерных устройствах хранения данных.

[0008] Эти и другие реализации необязательно могут включать в себя один или более следующих признаков: транзакция выполняется между счетом, ассоциированным с первым узлом, и счетом, ассоциированным со вторым узлом, и способ дополнительно содержит обновление, после определения того, что транзакция является достоверной, счета первого узла и счета второго узла на основе суммы транзакции и сдачи; каждый из множества активов ассоциирован с одним или более из типа активов, стоимости активов, скрытой в фиксации, и случайного числа, используемого для формирования

фиксации; определение того, что каждый из множества активов ассоциирован с идентичным типом активов; первая фиксация, вторая фиксация и фиксация, которая скрывает стоимость активов, формируются на основе схемы фиксации, которая является гомоморфной, при этом определение того, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи, выполняется на основе гомоморфизма схемы фиксации; линейная детерминированная HE-схема извлекается из вероятностной HE-схемы на основе изменения случайного числа, ассоциированного с вероятностной HE-схемой, на фиксированное число; ZKP содержит фиксацию, которая скрывает пятое случайное число и шестое случайное число, шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа второго счета на основе линейной детерминированной HE-схемы, и шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа первого счета на основе линейной детерминированной HE-схемы; ZKP формируется и используется для определения того, что транзакция является достоверной, на основе свойств линейного детерминированного HE; определение того, что транзакция является достоверной, выполняется на основе ZKP без взаимодействий между первым узлом и вторым узлом через часть за пределами сети цепочек блоков.

[0009] Описание изобретения также предоставляет один или более энергонезависимых машиночитаемых носителей хранения данных, соединенных с одним или более процессоров и имеющих сохраненные инструкции, которые, при выполнении посредством одного или более процессоров, инструктируют одному или более процессоров выполнять операции в соответствии с реализациями способов, предусмотренных в данном документе.

[0010] Описание изобретения дополнительно предоставляет систему для реализации способов, предусмотренных в настоящем документе. Система включает в себя один или более процессоров и машиночитаемый носитель хранения данных, соединенный с одним или более процессоров, имеющий сохраненные инструкции, которые, при выполнении посредством одного или более процессоров, инструктируют одному или более процессоров выполнять операции в соответствии с реализациями способов, предусмотренных в данном документе.

[0011] Реализации предмета изобретения, описанного в этом подробном описании, могут реализовываться таким образом, чтобы реализовывать конкретные преимущества или технические эффекты. Например, реализации описания изобретения разрешают балансу счета и сумме транзакции узлов цепочки блоков быть закрытыми во время транзакций. Получатель перевода денежных средств не должен обязательно подтверждать транзакцию или использовать случайное число для того, чтобы верифицировать фиксацию, проверка достоверности транзакций может быть неинтерактивной. Узел цепочки блоков может проверять достоверность транзакции на основе HE и схем фиксации, чтобы обеспечивать возможность доказательства с нулевой передачей знаний.

[0012] Описанная технология разрешает повышение безопасности счетов/данных различного мобильного вычислительного устройства. Баланс счетов и суммы транзакций могут шифроваться на основе HE и скрываться посредством схем фиксации. В связи с этим, консенсусный узел может обновлять баланс счетов в реестре после транзакции на основе свойств HE без раскрытия фактического баланса счета для счета. Поскольку случайное число не должно обязательно отправляться получателю, чтобы подтверждать транзакцию, риск утечки данных может уменьшаться, и меньший объем вычислительных

ресурсов и ресурсов запоминающего устройства должен использоваться для того, чтобы управлять случайным числом.

[0013] Следует принимать во внимание, что способы в соответствии с описанием изобретения могут включать в себя любую комбинацию аспектов и признаков, описанных в данном документе. Таким образом, способы в соответствии с описанием изобретения не ограничены комбинациями аспектов и признаков, конкретно описанными в данном документе, но также включают в себя любую предоставленную комбинацию аспектов и признаков.

[0014] Подробности одной или более реализаций описания изобретения изложены на прилагаемых чертежах и в нижеприведенном описании. Другие признаки и преимущества описания изобретения должны становиться очевидными из описания и чертежей, а также из формулы изобретения.

Описание чертежей

[0015] Фиг. 1 иллюстрирует пример окружения, которое может использоваться для того, чтобы выполнять реализации описания изобретения.

[0016] Фиг. 2 иллюстрирует пример концептуальной архитектуры в соответствии с реализациями описания изобретения.

[0017] Фиг. 3 иллюстрирует пример процесса проверки достоверности с защитой конфиденциальности транзакции с цепочками блоков на основе гомоморфного шифрования.

[0018] Фиг. 4 иллюстрирует пример транзакции с цепочками блоков в соответствии с реализациями описания изобретения.

[0019] Фиг. 5 иллюстрирует другой пример процесса проверки достоверности с защитой конфиденциальности транзакции с цепочками блоков на основе гомоморфного шифрования.

[0020] Фиг. 6 иллюстрирует пример способа, который может осуществляться в соответствии с реализациями описания изобретения.

[0021] Фиг. 7 иллюстрирует другой пример способа, который может осуществляться в соответствии с реализациями описания изобретения.

[0022] Фиг. 8 иллюстрирует пример узла цепочки блоков, который может выполнять процесс в соответствии с реализациями описания изобретения.

[0023] Аналогичные ссылки с номерами на различных чертежах указывают аналогичные элементы.

Подробное описание изобретения

[0024] Реализации описания изобретения включают в себя машинореализованные способы для неинтерактивных верификаций с сохранением конфиденциальности транзакций с цепочками блоков. Более конкретно, реализации описания изобретения направлены на машинореализованный способ, допускающий параллельную проверку достоверности нескольких транзакций, ассоциированных со счетом узла цепочки блоков, на основе схем фиксации и гомоморфного шифрования без раскрытия конфиденциальной информации, такой как сумма транзакции, баланс счетов или случайные числа для формирования фиксаций, для других узлов цепочки блоков. В некоторых реализациях, действия включают в себя прием данных транзакции, ассоциированных с транзакцией, причем данные транзакции содержат: данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, вычисленную на основе удержания суммы транзакции из полной стоимости множества активов, сумму транзакции и третье случайное число, оба из которых шифруются

посредством открытого ключа второго узла на основе линейной детерминированной схемы гомоморфного шифрования (HE), сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе линейной детерминированной HE-схемы, одно или более доказательств по диапазону, доказательство с нулевой передачей знаний (ZKP) и цифровую подпись, сформированную на основе закрытого ключа, соответствующего открытому ключу первого узла; верификацию цифровой подписи на основе открытого ключа первого узла; определение того, что одно или более доказательств по диапазону доказывают то, что сумма транзакции и сдача больше или равны нулю; определение того, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи; и определение, на основе ZKP, того, что транзакция является достоверной, посредством определения того, что первое случайное число равно третьему случайному числу, второе случайное число равно четвертому случайному числу, и сумма транзакции, скрытая в первой фиксации, равна сумме транзакции, зашифрованной посредством открытого ключа второго узла. Другие реализации включают в себя соответствующие системы, оборудование и компьютерные программы, выполненные с возможностью выполнять действия способов, кодированных на компьютерных устройствах хранения данных.

[0025] Чтобы предоставлять дополнительный контекст для реализаций описания изобретения, и как представлено выше, системы распределенных реестров (DLS), которые также могут упоминаться как консенсусные сети (например, состоящие из узлов между равноправными узлами) и сети цепочек блоков, позволяют участвующим объектам защищенно и неизменно проводить транзакции и сохранять данные. Цепочка блоков используется в данном документе, чтобы, в общем, означать DLS независимо от конкретных вариантов использования.

[0026] Цепочка блоков представляет собой структуру данных, которая сохраняет транзакции таким способом, что транзакции являются неизменными и могут впоследствии верифицироваться. Цепочка блоков включает в себя один или более блоков. Каждый блок в цепочке сразу связывается с предыдущим блоком перед ним в цепочке посредством включения криптографического хэша предыдущего блока. Каждый блок также включает в себя временную метку, собственный криптографический хэш и одну или более транзакций. Транзакции, которые уже верифицированы посредством узлов сети цепочек блоков, хэшируются и кодируются в дерево Меркла. Дерево Меркла представляет собой структуру данных, в которой данные в концевых узлах дерева хэшируются, и все хэши в каждой ветви дерева конкатенируются в корне ветви. Этот процесс продолжает дерево вплоть до корня всего дерева, которое сохраняет хэш, который представляет все данные в дереве. Хэш, подразумеваемый в качестве транзакции, сохраненной в дереве, может быстро верифицироваться посредством определения то, является или нет оно согласованным со структурой дерева.

[0027] Исходя из того, что цепочка блоков представляет собой структуру данных для сохранения транзакций, сеть цепочек блоков представляет собой сеть вычислительных узлов, которые управляют, обновляют и поддерживают одну или более цепочек блоков. Как представлено выше, сеть цепочек блоков может предоставляться в качестве открытой сети цепочек блоков, закрытой сети цепочек блоков или консорциальной сети цепочек блоков.

[0028] В открытой цепочке блоков, консенсусный процесс управляется посредством узлов консенсусной сети. Например, сотни, тысячи, даже миллионы объектов могут участвовать в открытой цепочке блоков, каждый из которых управляет, по меньшей мере, одним узлом в открытой цепочке блоков. Соответственно, открытая цепочка

блоков может считаться открытой сетью относительно участвующих объектов. В некоторых примерах, большинство объектов (узлов) должны подписывать каждый блок для того, чтобы блок был достоверным и добавлялся в цепочку блоков. Примерные открытые сети цепочек блоков включают в себя конкретные платежные сети между равноправными узлами, которые используют распределенный реестр, называемый "цепочкой блоков". Тем не менее, как отмечено выше, термин "цепочка блоков" используется для того, чтобы, в общем, означать распределенные реестры без конкретной ссылки на конкретные сети цепочек блоков.

[0029] В общем, открытая цепочка блоков поддерживает открытые транзакции. Открытая транзакция совместно используется со всеми узлами в цепочке блоков, и цепочка блоков реплицируется по всем узлам. Таким образом, все узлы находятся в идеальном консенсусе состояния относительно цепочки блоков. Чтобы достигать консенсуса (например, соглашения с добавлением блока в цепочку блоков), консенсусный протокол реализуется в сети цепочек блоков. Примерные консенсусные протоколы включают в себя, без ограничения, доказательство выполнения работы (POW), доказательство доли владения (POS) и доказательство наличия полномочий (POA). POW упоминается дополнительно в данном документе в качестве неограничивающего примера.

[0030] Реализации описания изобретения включают в себя машинореализованные способы для неинтерактивных верификаций с сохранением конфиденциальности транзакций с цепочками блоков. Более конкретно, реализации описания изобретения направлены на машинореализованный способ, допускающий параллельную проверку достоверности нескольких транзакций, ассоциированных со счетом узла цепочки блоков, на основе схем фиксации и гомоморфного шифрования без раскрытия конфиденциальной информации, такой как сумма транзакции, баланс счетов или случайные числа для формирования фиксаций, для других узлов цепочки блоков.

[0031] Согласно реализациям описания изобретения, узлы цепочки блоков могут использовать общую модель на основе счетов, которая может поддерживать параллельную верификацию транзакций в качестве способа ведения записей. По сравнению с моделью на основе баланса счетов, узлы цепочки блоков, которые приспосабливают общую модель на основе счетов, ведут записи множества активов вместо баланса счетов. Каждый из множества активов может быть ассоциирован, по меньшей мере, с одним из типа активов, идентификатора актива или стоимости активов. Актив согласно общей модели на основе счетов может иметь любую форму или тип, к примеру, денежный или фиксированный. Денежные активы могут включать в себя реальную валюту или криптовалюту. В некоторых реализациях, фиксированные активы могут конвертироваться в денежные активы, ассоциированные с денежной суммой. Денежная сумма затем может использоваться для того, чтобы выполнять транзакции между счетами сети цепочек блоков. В качестве иллюстрации, предполагается, что активы, описанные в реализациях описания изобретения, конвертируются в идентичный тип валюты и сохраняются на счетах цепочек блоков согласно общей модели на основе счетов.

[0032] Чтобы защищать конфиденциальность данных, транзакции могут записываться в цепочку блоков (реестр) на основе фиксации без раскрытия информации сумм транзакций или денежных сумм, ассоциированной со счетами пользователей цепочек блоков. Схема фиксации может использоваться для того, чтобы формировать фиксацию суммы транзакции с использованием случайного числа. Примерная схема фиксации включает в себя, без ограничения, PC-схему. Поскольку сумма транзакции скрывается

в фиксации, одно или более доказательств по диапазону могут использоваться для того, чтобы доказывать то, что сумма транзакции не превышает стоимость счета пользователя цепочек блоков.

[0033] Согласно модели на основе баланса счетов, доказательства по диапазону ассоциированы с балансом счета. Если проведено более одной транзакции, но не все транзакции проходят проверку достоверности и записываются в цепочке блоков, доказательства по диапазону могут быть ассоциированы с некорректным балансом счетов, в силу чего могут быть недопустимыми. Для сравнения, согласно общей модели на основе счетов, стоимость счета может вычисляться как суммарная величина множества активов. Когда сумма транзакции должна переводиться между счетами пользователей цепочек блоков, по меньшей мере, часть из множества активов с комбинированной стоимостью, большей или равной сумме транзакции, может использоваться для того, чтобы покрывать сумму транзакции. Дополнительные переводы могут осуществляться при таком условии, что оставшиеся активы имеют комбинированную стоимость, большую суммы, которая должна переводиться. Даже если транзакции не проходят проверку достоверности и записываются в цепочке блоков, доказательства по диапазону, показывающие то, что комбинированная стоимость оставшихся активов превышает или равна сумме транзакции, по-прежнему могут быть достоверным. Следовательно, более одной верификации транзакций могут выполняться параллельно согласно общей модели на основе счетов.

[0034] Согласно реализациям описания изобретения, транзакции с цепочками блоков могут проходить проверку достоверности и записываться в цепочку блоков (реестр) на основе фиксации без раскрытия баланса счета транзакции, суммы транзакции или случайного числа, используемого для того, чтобы формировать фиксацию. Схема фиксации, такая как PC-схема, может использоваться для того, чтобы формировать фиксацию суммы транзакции на основе случайного числа. Сумма транзакции и случайное число могут шифроваться с использованием вероятностного или линейного детерминированного HE. Сумма транзакции и случайное число также могут использоваться для того, чтобы формировать набор значений в качестве ZKP для проверки достоверности транзакции на основе свойств используемой HE-схемы. Фиксация суммы транзакции, зашифрованная сумма транзакции и случайное число и ZKP могут использоваться посредством узла цепочки блоков для того, чтобы верифицировать то, является или нет транзакция достоверной, без раскрытия баланса счетов, суммы транзакции или случайного числа.

[0035] Фиг. 1 иллюстрирует пример окружения 100, которое может использоваться для того, чтобы выполнять реализации описания изобретения. В некоторых примерах, примерное окружение 100 обеспечивает возможность объектам участвовать в открытой цепочке 102 блоков. Примерное окружение 100 включает в себя вычислительные системы 106, 108 и сеть 110. В некоторых примерах, сеть 110 включает в себя локальную вычислительную сеть (LAN), глобальную вычислительную сеть (WAN), Интернет либо комбинацию вышеозначенного и соединяет веб-узлы, пользовательские устройства (например, вычислительные устройства) и внутренние интерфейсные системы. В некоторых примерах, к сети 110 может осуществляться доступ по линии проводной и/или беспроводной связи.

[0036] В проиллюстрированном примере, каждая вычислительная система 106, 108 может включать в себя любую соответствующую вычислительную систему, которая обеспечивает участие в качестве узла в открытой цепочки 102 блоков. Примерные вычислительные устройства включают в себя, без ограничения, сервер, настольный

компьютер, переносной компьютер, планшетное вычислительное устройство и смартфон. В некоторых примерах, вычислительные системы 106, 108 выполняют хостинг одной или более машинореализованных услуг для взаимодействия с открытой цепочкой 102 блоков. Например, вычислительная система 106 может выполнять хостинг машинореализованных услуг первого объекта (например, пользователя A), к примеру, системы управления транзакциями, которую использует первый объект для того, чтобы управлять своими транзакциями с одним или более других объектов (например, других пользователей). Вычислительная система 108 может выполнять хостинг машинореализованных услуг второго объекта (например, пользователя B), к примеру, система управления транзакциями, которую использует второй объект для того, чтобы управлять своими транзакциями с одним или более других объектов (например, других пользователей). В примере по фиг. 1, открытая цепочка 102 блоков представляется как сеть с равноправными узлами узлов, и вычислительные системы 106, 108 предоставляют узлы первого объекта и второго объекта, соответственно, которые участвуют в открытой цепочке 102 блоков.

[0037] Фиг. 2 иллюстрирует пример концептуальной архитектуры 200 в соответствии с реализациями описания изобретения. Примерная концептуальная архитектура 200 включает в себя уровень 202 объектов, уровень 204 предоставления размещенных услуг и уровень 206 открытых цепочек блоков. В проиллюстрированном примере, уровень 202 объектов включает в себя три объекта, объект_1 (E1), объект_2 (E2) и объект_3 (E3), причем каждый объект имеет соответствующую систему 208 управления транзакциями.

[0038] В проиллюстрированном примере, уровень 204 предоставления размещенных услуг включает в себя интерфейсы 210 цепочек блоков для каждой системы 208 управления транзакциями. В некоторых примерах, соответствующая система 208 управления транзакциями обменивается данными с соответствующим интерфейсом 210 цепочек блоков по сети (например, по сети 110 по фиг. 1) с использованием протокола связи (например, протокола защищенной передачи гипертекста (HTTPS)). В некоторых примерах, каждый интерфейс 210 цепочек блоков предоставляет соединение связи между соответствующей системой 208 управления транзакциями и уровнем 206 цепочек блоков. Более конкретно, каждый интерфейс 210 цепочек блоков обеспечивает возможность соответствующему объекту проводить транзакции, записываемые в сети 212 цепочек блоков уровня 206 цепочек блоков. В некоторых примерах, связь между интерфейсом 210 цепочек блоков и уровнем 206 цепочек блоков проводится с использованием удаленных вызовов процедур (RPC). В некоторых примерах, интерфейсы 210 цепочек блоков "выполняют хостинг" узлов цепочек блоков для соответствующих систем 208 управления транзакциями. Например, интерфейсы 210 цепочек блоков предоставляют интерфейс прикладного программирования (API) для доступа к сети 212 цепочек блоков.

[0039] Как описано в данном документе, сеть 212 цепочек блоков предоставляется в качестве сети с равноправными узлами, включающей в себя множество узлов 214, которые неизменно записывают информацию в цепочку 216 блоков. Хотя одна цепочка 216 блоков схематично проиллюстрирована, несколько копий цепочки 216 блоков предоставляются и поддерживаются в сети 212 цепочек блоков. Например, каждый узел 214 сохраняет копию цепочки 216 блоков. В некоторых реализациях, цепочка 216 блоков сохраняет информацию, ассоциированную с транзакциями, которые выполняются между двумя или более объектов, участвующих в открытой цепочке блоков.

[0040] Фиг. 3 иллюстрирует пример процесса 300 проверки достоверности с защитой

конфиденциальности транзакции с цепочками блоков на основе HE. На высоком уровне, процесс 300 осуществляется посредством пользовательского узла A 302, пользовательского узла B (не показан на фиг. 3) и узла 304 цепочки блоков, также называемого "консенсусным узлом". Как счет пользовательского узла A 302, так и счет пользовательского узла B могут иметь модель ведения записей на основе общей модели на основе счетов. Таким образом, записи счетов пользовательского узла A 302 и пользовательского узла B сохраняются в качестве множества активов. Транзакция, такая как перевод стоимости, может проводиться из пользовательского узла A 302 в пользовательский узел B. Пользовательский узел A 302 может выбирать один или более активов счета, которые имеют полную стоимость, большую или равную сумме транзакции для того, чтобы покрывать транзакцию. Разность между полной стоимостью одного или более активов и суммой транзакции может рассматриваться как сдача транзакции, остающаяся для пользовательского узла A 302.

[0041] Чтобы защищать конфиденциальность счета, пользовательский узел A 302 может формировать фиксации стоимостей активов, используемых для того, чтобы покрывать транзакцию. Пользовательский узел A 302 также может формировать фиксацию суммы транзакции для транзакции. Пользовательский узел A 302 также может использовать HE, чтобы шифровать сумму транзакции, сдачу и случайные числа, используемые для того, чтобы формировать фиксации. Чтобы верифицировать достоверность транзакции, узел 304 цепочки блоков может сравнивать сумму транзакции, сдачу и случайные числа, скрытые в фиксациях и зашифрованные посредством HE на основе ZKP. Если сумма транзакции, сдача и случайные числа совпадают, транзакция определяется в качестве достоверной посредством узла 304 цепочки блоков. Дополнительные сведения по процессу 300 пояснены в нижеприведенном описании по фиг. 3.

[0042] На 306, пользовательский узел A 302 выбирает множество активов для перевода суммы транзакции в пользовательский узел B. Пользовательский узел A 302 и пользовательский узел B могут представлять собой консенсусные узлы цепочки блоков или пользовательские узлы, которые используют сеть цепочек блоков без участия в консенсусном процессе. Как пояснено выше, пользовательский узел A 302 может использовать общую модель на основе счетов для того, чтобы вести записи. Вместо ведения баланса счета для записи согласно модели на основе баланса счетов, стоимость счета пользовательского узла A 302 измеряется посредством полной стоимости активов, которые он обрабатывает. Пользовательский узел A 302 может выбирать множество активов, которые имеют достаточную стоимость для того, чтобы покрывать сумму транзакции. Например, если сумма транзакции составляет 7,5 долларов США, пользовательский узел A 302 может выбирать три актива, которые стоят 5, 2 и 1 доллар США, соответственно, для того, чтобы покрывать сумму транзакции.

[0043] В некоторых реализациях, каждый актив может быть ассоциирован с адресом транзакции или идентификатором актива, который идентифицирует соответствующий актив. Идентификатор актива может представлять собой хэширование информации активов. Идентификаторы активов для k выбранных активов могут представляться как ID_1,..., ID_k.

[0044] На 308, пользовательский узел A 302 вычисляет сдачу на основе полной стоимости множества активов и суммы транзакции. Поскольку активы выбираются таким образом, чтобы иметь полную стоимость, превышающую сумму транзакции, сдача может вычисляться как полная стоимость выбранных активов, из которой удержана сумма транзакции. С использованием t для того, чтобы представлять сумму

транзакции, и t_0 для того, чтобы представлять сдачу, вычисление сдачи может выражаться как $t_0=a_1+...+a_k-t$, где $a_1,..., a_k$ являются, соответственно, стоимостями активов k активов, выбранных посредством пользовательского узла A 302, чтобы покрывать сумму t транзакции.

[0045] На 310, пользовательский узел A 302 формирует случайное число, соответствующее сумме транзакции, и случайное число, соответствующее сдаче. Случайное число, соответствующее сумме t транзакции, может обозначаться как r. Случайное число, соответствующее сдаче t_0, может обозначаться как r_0. В некоторых реализациях, могут формироваться множество случайных чисел, чтобы формировать фиксации стоимостей активов. Например, предположим, что $a_1,..., a_k$ являются стоимостями активов, и случайные числа, которые соответствуют стоимостям активов, могут выражаться как $r_{a1},..., r_{ak}$.

[0046] В некоторых реализациях, случайное число r_0 может вычисляться вместо случайно сформированного. Вычисление может выражаться как $r_0=r_{a1}+...+r_{ak-r}$, где r является случайным числом, сформированным с возможностью формировать фиксацию для суммы t транзакции. Посредством использования вычисленного случайного числа r_0, пользовательский узел A 302 не должен формировать дополнительное ZKP, чтобы доказывать то, что полная стоимость переведенных активов равна полной стоимости принимаемых активов. В некоторых реализациях, другое случайное число r' может вычисляться как $r'=r_1+...+r_{k-r}-r_0$, чтобы помогать с ZKP.

[0047] На 312, пользовательский узел A 302 формирует фиксации суммы транзакции и сдачи и шифрует соответствующие случайные числа на основе вероятностного HE. В некоторых реализациях, гомоморфные схемы фиксации, такие как PC, могут использоваться для того, чтобы формировать фиксации. С использованием PC в качестве неограничивающего примера, PC суммы t транзакции может формироваться посредством использования случайного числа r, которое может выражаться как $PC(r, t)=g^r h^t$, где g и h могут быть генераторами эллиптической кривой, и PC(r, t) является скалярным умножением точек кривой. Аналогично, PC сдачи t_0 может выражаться как $PC(r_0, t_0)=g^{r0}h^{t0}$.

[0048] Случайное число r может шифроваться с использованием открытого ключа пользовательского узла B на основе вероятностной HE-схемы, такой как схема шифрования Окамото-Учиямы (OU). Следует понимать, что также могут использоваться другие HE-схемы, такие как схема Бонеха-Го-Ниссима. С использованием OU в качестве неограничивающего примера, случайное число может шифроваться на основе OU посредством трактовки суммы t транзакции в качестве случайного числа, которое может выражаться как $OU_B(r, t)=u^r v^t$ или просто $OU_B(t)$, где u является генератором $(Z/nZ)^*$, удовлетворяющее таким условиям, что $v=u^n \bmod n$, и $n=p \times q$, где p и q являются двумя простыми числами. Вероятностная OU может удовлетворять такому свойству, что $OU(a+b)=OU(a)*OU(b)$, где a и b являются простым текстом, используемым для OU.

[0049] Случайное число r_0 может шифроваться с использованием открытого ключа пользовательского узла A 302. Случайное число может шифроваться на основе OU посредством трактовки сдачи t_0 в качестве случайного числа, которое может выражаться как $OU_A(r_0, t_0)$.

[0050] Шифрованный текст суммы транзакции затем может выражаться как T=(PC

(t, r), $OU_B(r, t)$), и шифрованный текст сдачи может выражаться как $T_0=(PC(t_0, r_0), OU_A(r_0, t_0))$. Аналогично, шифрованный текст k выбранных активов может выражаться как $T_i=(PC(t_i, r_i), OU_A(r_i, t_i))$, где i=1,..., k.

[0051] На 314, пользовательский узел A 302 формирует одно или более доказательств по диапазону. В некоторых реализациях, первое доказательство по диапазону, RP_1, может формироваться для того, чтобы показывать то, что сумма транзакции $t\geq 0$. Второе доказательство по диапазону, RP_2, может формироваться для того, чтобы показывать то, что сдача $t_0\geq 0$, или другими словами, то, что полная стоимость множества активов превышает или равна сумме транзакции.

[0052] На 316, пользовательский узел A 302 формирует ZKP. ZKP может использоваться для того, чтобы показывать то, что случайное число и сумма транзакции, скрытая в PC(r, t), являются идентичными случайному числу и сумме транзакции, зашифрованной в $OU_B(r, t)$, и случайное число и сумма транзакции, скрытая в $PC(r_0, t_0)$, являются идентичными случайному числу и сумме транзакции, зашифрованной в $OU_A(r_0, t_0)$. Чтобы формировать ZKP, два случайных числа t'_1 и r'_1 могут выбираться. Два случайных числа могут использоваться для того, чтобы формировать три значения, которые составляют $P=PC(t'_1, r'_1)$, $P'= OU_B(r'_1, t'_1)$, $P''= OU_A(r'_1, t'_1)$. Три значения затем могут использоваться для того, чтобы формировать хэш, выражаемый как x=Hash(P, P', P''). Хэш-значение x может использоваться для того, чтобы вычислять $t'_2=t'_1+xt$, $r'_2=r'_1+xr$, $t'_3=t'_1+xt$ и $r'_3=r'_1+xr_0$. ZKP затем может выражаться как $(P, P', t'_2, r'_2, P'', t'_3, r'_3)$.

[0053] На 318, пользовательский узел A 302 использует закрытый ключ для того, чтобы формировать цифровую подпись с тем, чтобы подписывать данные транзакции. В некоторых реализациях, данные транзакции могут включать в себя идентификаторы активов для k выбранных активов (ID_1,..., ID_k), шифрованный текст суммы транзакции (T), шифрованный текст сдачи (T_0), доказательства по диапазону (RP_1 и RP_2), случайное число r' и ZKP.

[0054] На 320, пользовательский узел A 302 предоставляет копию с цифровой подписью данных транзакции в сеть цепочек блоков.

[0055] На 322, узел 304 цепочки блоков верифицирует цифровую подпись. Верификация цифровой подписи может выполняться для того, чтобы обеспечивать то, что данные транзакции отправляются посредством пользовательского узла A 302. В некоторых реализациях, узел 304 цепочки блоков включает в себя механизм защиты от двойной траты, который может верифицировать то, выполнена уже транзакция или нет. Если да, узел 304 цепочки блоков может отклонять транзакцию.

[0056] На 324, узел 304 цепочки блоков верифицирует то, ассоциированы или нет выбранные активы со счетом пользовательского узла A. Верификация может быть основана на идентификаторах активов для активов.

[0057] На 326, узел 304 цепочки блоков верифицирует то, что полная стоимость выбранного множества активов равна суммарной величине суммы транзакции и сдачи. Другими словами, цепочка блоков верифицирует то, что $a_1+...+a_k=t+t_0$. Как пояснено выше, согласно общей модели на основе счетов, активы могут сохраняться в цепочке блоков в качестве PC, чтобы защищать конфиденциальность данных. На основе гомоморфизма PC, $PC(r_{a1}, a_1)$ x.. x $PC(r_{ak}, a_k)=PC(r_{a1}+...+ r_{ak}, a_1+...+a_k)$ и PC(r, t) x $PC(r_0, t_0)=PC(r+r_0, t+t_0)$. Следовательно, посредством показа того, что $PC(r_{a1}, a_1)$ x... x $PC(r_{ak}$,

$a_k)=PC(r, t) \times PC(r_0, t_0) \times g^{r'}$, можно доказывать то, что $a_1+...+a_k=t+t_0$.

[0058] На 328, узел 304 цепочки блоков верифицирует одно или более доказательств по диапазону.

[0059] На 330, узел 304 цепочки блоков верифицирует ZKP. Как пояснено выше, ZKP может формироваться, чтобы верифицировать то, является или нет случайное число, соответствующее сумме транзакции, зашифрованной с использованием открытого ключа пользовательского узла B, идентичным соответствующему случайному числу, скрытому посредством PC, и то, является или нет случайное число, соответствующее сдаче, зашифрованной с использованием открытого ключа пользовательского узла A 302, идентичным соответствующему случайному числу, скрытому посредством PC. В некоторых реализациях, чтобы верифицировать ZKP, узел 304 цепочки блоков может сначала вычислять хэш-значение x в качестве x=Hash(P, P', P''). Узел 304 цепочки блоков затем может верифицировать то, являются или нет $PC(t'_2, r'_2)=P \times PC(t, r)^x$, $OU_B(r'_2, t'_2)=P' \times OU_B(r, t)^x$, $PC(t'_3, r'_3)=P \times PC(t_0, r_0)^x$ and $OU_A(r'_3, t'_3)=P'' \times OU_A(r_0, t_0)^x$ истинными. Если все являются истинными, примерный процесс 300 переходит к 332. В противном случае, узел 304 цепочки блоков может отклонять транзакцию.

[0060] На 332, узел 304 цепочки блоков обновляет счета пользовательского узла A 302 и пользовательского узла B. Поскольку счета пользовательского узла A 302 и пользовательского узла B сохраняют активы в качестве записей согласно общей модели на основе счетов, после транзакции, множество активов, переведенных с пользовательского узла A 302, может удаляться со счета пользовательского узла A 302. Сдача может добавляться обратно на счет пользовательского узла A 302. Сумма транзакции и соответствующий идентификатор актива могут добавляться в качестве нового актива на счет пользовательского узла B. В некоторых реализациях, обновление может выполняться на основе обновления списков активов, поддерживаемых посредством соответствующих счетов пользовательского узла A 302 и пользовательского узла B. В некоторых реализациях, обновление может выполняться на основе добавления шифрованных текстов суммы транзакции и сдачи зашифрованных стоимостей активов, поддерживаемых посредством пользовательского узла A 302 и пользовательского узла B. В дальнейшем в данном документе подробнее описывается обновление счетов со ссылкой на фиг. 4.

[0061] Фиг. 4 иллюстрирует пример транзакции 400 с цепочками блоков в соответствии с реализациями описания изобретения. Как показано в примерной транзакции 400 с цепочками блоков, пользовательский узел A 402 переводит сумму t транзакции в пользовательский узел B 404. Перед транзакцией, пользовательский узел A 402 имеет n активов, включающих в себя (ID_1, T_1), (ID_2, T_2), (ID_n, T_n).

[0062] С использованием схем фиксации, схем шифрования и процесса проведения транзакций, описанного в данном документе со ссылкой на фиг. 3, в качестве примера, пользовательский узел A 402 может формировать данные 408 транзакции, которые могут включать в себя идентификаторы активов для k выбранных активов, ID, ID_2,..., ID_k. Данные 408 транзакции дополнительно могут включать в себя T_0, T, RP_1, RP_2, r' и ZKP. После того, как данные 408 транзакции формируются, пользовательский узел A 402 может добавлять свою цифровую подпись и предоставлять данные транзакции с цифровой подписью в сеть 406 цепочек блоков для консенсуса.

[0063] После транзакции, выбранные активы k могут удаляться со счета актива пользователя 402. Сдача может добавляться обратно в пользовательский узел A 402.

Следовательно, пользовательский узел A 402 может иметь следующие активы, выражаемые как (ID_{k+1}, T_{k+1}), (ID_{k+2}, T_{k+2}),..., (ID_n, T_n), (ID_0, T_0), где ID_0 представляет идентификатор актива сдачи t_0.

[0064] Перед транзакцией, пользовательский узел B 404 имеет m активов, которые могут выражаться как ($ID_{1'}$, $T_{1'}$), ($ID_{2'}$, $T_{2'}$), ($ID_{m'}$, $T_{m'}$). После транзакции, сумма транзакции может добавляться в пользовательский узел B 404. Пользовательский узел B 404 может иметь следующие активы, выражаемые как ($ID_{1'}$, $T_{1'}$), ($ID_{2'}$, $T_{2'}$), ($ID_{m'}$, $T_{m'}$), ($ID_{T,\ T}$), где ID_T представляет идентификатор актива суммы t транзакции.

[0065] Фиг. 5 иллюстрирует пример процесса 500 проверки достоверности с защитой конфиденциальности транзакции с цепочками блоков на основе HE. На высоком уровне, примерный процесс 500 осуществляется посредством пользовательского узла A 502, пользовательского узла B (не показан на фиг. 5) и узла 504 цепочки блоков, также называемого "консенсусным узлом". Как счет пользовательского узла A 502, так и счет пользовательского узла B могут быть основаны на общей модели на основе счетов. Транзакция, такая как перевод стоимости, может проводиться из пользовательского узла A 502 в пользовательский узел B. Пользовательский узел A 502 может выбирать один или более активов счета, которые имеют полную стоимость, большую или равную сумме транзакции для того, чтобы покрывать транзакцию. Разность между полной стоимостью одного или более активов и суммой транзакции может рассматриваться как сдача транзакции, остающаяся для пользовательского узла A 502.

[0066] Чтобы защищать конфиденциальность счета, пользовательский узел A 502 может формировать фиксации стоимостей активов, используемых для того, чтобы покрывать транзакцию, и суммы по транзакции с использованием схемы фиксации, такой как PC. Пользовательский узел A 502 также может использовать линейное детерминированное HE, чтобы шифровать случайные числа, используемые для того, чтобы формировать фиксации. Линейное детерминированное HE может иметь следующие свойства: HE(s+t)=HE x HE(t) и HE(kt)=$HE(t)^k$. Чтобы верифицировать достоверность транзакции, узел 504 цепочки блоков может сравнивать случайные числа, скрытые в фиксации и зашифрованные посредством HE на основе ZKP. Если случайные числа совпадают, транзакция может определяться как достоверная посредством узла 504 цепочки блоков. Дополнительные сведения по примерному процессу 500 пояснены в нижеприведенном описании по фиг. 5

[0067] На 506, пользовательский узел A 502 выбирает множество активов для перевода суммы транзакции в пользовательский узел B. Пользовательский узел A 502 и пользовательский узел B могут представлять собой консенсусный узел цепочки блоков или пользовательские узлы, которые используют сеть цепочек блоков без участия в консенсусном процессе. Пользовательский узел A 502 может выбирать множество активов, которые имеют достаточную стоимость для того, чтобы покрывать сумму транзакции.

[0068] В некоторых реализациях, каждый актив может быть ассоциирован с адресом транзакции или идентификатором актива, который идентифицирует соответствующий актив. Идентификатор актива может представлять собой хэширование информации активов. Идентификаторы активов для k выбранных активов могут представляться как ID_1,..., ID_k.

[0069] На 508, пользовательский узел A 502 вычисляет сдачу на основе полной стоимости множества активов и суммы транзакции. Поскольку активы выбираются таким образом, чтобы иметь полную стоимость, превышающую сумму транзакции,

сдача может вычисляться как полная стоимость выбранных активов, из которой удержана сумма транзакции. С использованием t для того, чтобы представлять сумму транзакции, и t_0 для того, чтобы представлять сдачу, вычисление сдачи может выражаться как $t_0=a_1+...+a_k-t$, где $a_1,..., a_k$ являются, соответственно, стоимостями активов k активов, выбранных посредством пользовательского узла A 502, чтобы покрывать сумму t транзакции.

[0070] На 510, пользовательский узел A 502 формирует случайное число, соответствующее сумме транзакции, и случайное число, соответствующее сдаче. Случайное число, соответствующее сумме t транзакции, может обозначаться как r. Случайное число, соответствующее сдаче t_0, может обозначаться как r_0. В некоторых реализациях, могут формироваться множество случайных чисел, чтобы формировать фиксации стоимостей активов. Например, предположим, что $a_1,..., a_k$ являются стоимостями активов, и случайные числа, которые соответствуют стоимостям активов, могут выражаться как $r_{a1},..., r_{ak}$.

[0071] В некоторых реализациях, случайное число r_0 может вычисляться вместо случайно сформированного. Вычисление может выражаться как $r_0= r_{a1}+...+r_{ak}-r$, где r является случайным числом, сформированным с возможностью формировать фиксацию для суммы t транзакции. Посредством вычисления r_0, пользовательский узел A 502 не должен формировать дополнительное ZKP, чтобы показывать то, что полная стоимость переведенных активов равна полной стоимости принимаемых активов. В некоторых реализациях, случайное число r' может вычисляться как $r'=r_1+...+r_k-r-r_0$.

[0072] На 512, пользовательский узел A 502 формирует фиксации суммы транзакции и сдачи и шифрует соответствующие случайные числа на основе детерминированного HE. В некоторых реализациях, гомоморфные схемы фиксации, такие как PC, могут использоваться для того, чтобы формировать фиксации. С использованием PC в качестве неограничивающего примера, PC суммы t транзакции может формироваться посредством использования случайного числа r, которое может выражаться как $PC(r, t)=g^r h^t$, где g и h могут быть генераторами эллиптической кривой, и PC(r, t) является скалярным умножением точек кривой. Аналогично, PC сдачи t_0 может выражаться как $PC(r_0, t_0)=g^{r0}h^{t0}$.

[0073] Случайное число r может шифроваться с использованием открытого ключа пользовательского узла B на основе линейного детерминированного HE. Линейное детерминированное HE может получаться из вероятностного HE, такого как HE Пэйе, HE Бенало, HE OU, HE Накаша-Штерна, HE Бонеха-Го-Ниссима, HE Дамгарда-Юрика или HE на основе равной вероятности, посредством фиксации случайного числа в HE-схеме равным 0 или 1 либо другому соответствующему числу. Зашифрованное случайное число может выражаться как HE(r).

[0074] Случайное число r_0 может шифроваться с использованием открытого ключа пользовательского узла A. Случайное число может шифроваться на основе линейного детерминированного HE. Зашифрованное случайное число может выражаться как $HE(r^0)$.

[0075] Шифрованный текст суммы t транзакции затем может выражаться как $T=(g^r h^t, HE_B(r))$, и шифрованный текст сдачи может выражаться как $T_0=(g^{r0}h^{t0}, HE_A(r_0))$.

Аналогично, шифрованный текст k выбранных активов может выражаться как $T_i=(g^{ri}h^{ti}$, $HE(r_i)$, где i=1,..., k.

[0076] На 514, пользовательский узел A 502 формирует одно или более доказательств по диапазону. В некоторых реализациях, первое доказательство по диапазону, RP_1, может формироваться для того, чтобы показывать то, что сумма транзакции $t\geq 0$. Второе доказательство по диапазону, RP_2, может формироваться для того, чтобы показывать то, что сдача $t_0\geq 0$, или другими словами, то, что полная стоимость множества активов превышает или равна сумме транзакции.

[0077] На 516, пользовательский узел A 502 формирует ZKP. ZKP может использоваться для того, чтобы показывать то, что, случайное число, скрытое в PC(r, t), является идентичным случайному числу, зашифрованному в HE(r), и случайное число, скрытое в $PC(r_0, t_0)$, является идентичным случайному числу, зашифрованному в HE (r0). Чтобы формировать ZKP, два случайных числа t'_1 и r'_1 могут выбираться. Два случайных числа могут использоваться для того, чтобы формировать три значения, которые составляют $P= g^{r'1}h^{t'1}$, $P'=HE_B(r'_1)$, $P''=HE_A(r'_1)$. Три значения затем могут использоваться для того, чтобы формировать хэш, выражаемый как x=Hash(P, P', P''). Хэш-значение x может использоваться для того, чтобы вычислять $t'_2=t'_1+xt$, $r'_2=r'_1+xr$, $t'_3=t'_1+xt$ и $r'_3=r'_1+xr_0$. ZKP затем может выражаться как (P, P', t'_2, r'_2, P'', t'_3, r'_3).

[0078] На 518, пользовательский узел A 502 использует закрытый ключ для того, чтобы формировать цифровую подпись с тем, чтобы подписывать данные транзакции. В некоторых реализациях, данные транзакции могут включать в себя идентификаторы активов для k выбранных активов (ID_1,..., ID_k), шифрованный текст суммы транзакции (T), шифрованный текст сдачи (T_0), доказательства по диапазону (RP_1 и RP_2), случайное число r' и ZKP.

[0079] На 520, пользовательский узел A 502 предоставляет копию с цифровой подписью данных транзакции в сеть цепочек блоков.

[0080] На 522, узел 504 цепочки блоков верифицирует цифровую подпись. Верификация цифровой подписи может выполняться для того, чтобы обеспечивать то, что данные транзакции отправляются посредством пользовательского узла A 502. В некоторых реализациях, узел 504 цепочки блоков включает в себя механизм защиты от двойной траты, который может верифицировать то, выполнена уже транзакция или нет. Если да, узел 504 цепочки блоков может отклонять транзакцию.

[0081] На 524, узел 504 цепочки блоков верифицирует то, ассоциированы или нет выбранные активы со счетом пользовательского узла A. Верификация может быть основана на идентификаторах активов для активов.

[0082] На 526, узел 504 цепочки блоков верифицирует то, что полная стоимость выбранного множества активов равна суммарной величине суммы транзакции и сдачи. Другими словами, узел 504 цепочки блоков верифицирует то, что $a_1+...+a_k=t+t_0$. Как пояснено выше, согласно общей модели на основе счетов, активы могут сохраняться в цепочке блоков в качестве PC, чтобы защищать конфиденциальность данных. На основе гомоморфизма PC, $PC(r_{a1}, a_1)$ x.. x $PC(r_{ak}, a_k)=PC(r_{a1}+...+ r_{ak}, a_1+...+a_k)$ и PC(r, t) x $PC(r_0, t_0)=PC(r+r_0, t+t_0)$. Следовательно, посредством показа того, что $PC(r_{a1}, a_1)$ x... x $PC(r_{ak}, a_k)=PC(r, t)$ x $PC(r_0, t_0)$ x $g^{r'}$, можно доказывать то, что $a_1+...+a_k=t+t_0$.

[0083] На 528, узел 504 цепочки блоков верифицирует одно или более доказательств

по диапазону.

[0084] На 530, узел 504 цепочки блоков верифицирует ZKP. Как пояснено выше, ZKP может формироваться, чтобы верифицировать то, является или нет случайное число, соответствующее сумме транзакции, зашифрованной с использованием открытого ключа пользовательского узла B, идентичным соответствующему случайному числу, скрытому посредством PC, и то, является или нет случайное число, соответствующее сдаче, зашифрованной с использованием открытого ключа пользовательского узла A 502, идентичным соответствующему случайному числу, скрытому посредством PC. В некоторых реализациях, чтобы верифицировать ZKP, узел 504 цепочки блоков может сначала вычислять хэш-значение x в качестве x=Hash(P, P', P''). Узел 504 цепочки блоков затем может верифицировать, являются или нет $g^{r'2}h^{t'2}=P \times (g^{r}h^{t})^{x}$, $HE_B(r')=P' \times HE(r)^{x}$, $g^{r'3}h^{t'3}=P \times (g^{r0}h^{t0})^{x}$, и $HE_A(r'_3)=P'' \times HE_A(r_0)^{x}$ истинными. Если каждое из них является истинным, примерный процесс 500 переходит к 532. В противном случае, узел 504 цепочки блоков может отклонять транзакцию.

[0085] На 532, узел 504 цепочки блоков обновляет счета пользовательского узла A 502 и пользовательского узла B. Поскольку счета пользовательского узла A 502 и пользовательского узла B сохраняют активы в качестве записей согласно общей модели на основе счетов, после транзакции, множество активов, переведенных с пользовательского узла A 502, могут удаляться со счета пользовательского узла A 502. Сдача может добавляться обратно на счет пользовательского узла A 502. Сумма транзакции и соответствующий идентификатор актива могут добавляться в качестве нового актива на счет пользовательского узла B. В некоторых реализациях, обновление может выполняться на основе обновления списков активов, поддерживаемых посредством соответствующих счетов пользовательского узла A 502 и пользовательского узла B. В некоторых реализациях, обновление может выполняться на основе добавления шифрованных текстов суммы транзакции и сдачи зашифрованных стоимостей активов, поддерживаемых посредством пользовательского узла A 502 и пользовательского узла B. Примерная транзакция 400 с цепочками блоков и соответствующие обновления счетов описываются в описании фиг. 4.

[0086] Фиг. 6 иллюстрирует пример процесса 600, который может выполняться в соответствии с реализациями описания изобретения. Для ясности представления, нижеприведенное описание, в общем, описывает способ 600 в контексте других чертежей в этом описании. Тем не менее, следует понимать, что примерный процесс 600 может выполняться, например, посредством любой системы, окружения, программного обеспечения и аппаратных средств либо комбинации систем, окружений, программного обеспечения и аппаратных средств, надлежащим образом. В некоторых реализациях, этапы примерного процесса 600 могут выполняться параллельно, в комбинации, циклически или в любом порядке.

[0087] На 602, консенсусный узел принимает данные транзакции, ассоциированные с транзакцией. В некоторых примерах, данные транзакции содержат данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, вычисленную на основе удержания суммы транзакции из полной стоимости множества активов, сумму транзакции и третье случайное число, оба из которых шифруются посредством открытого ключа второго узла на основе вероятностной HE-схемы, сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе

вероятностной HE-схемы, одно или более доказательств по диапазону, ZKP и цифровую подпись, сформированную на основе закрытого ключа, соответствующего открытому ключу первого узла.

[0088] В некоторых реализациях, каждый из множества активов ассоциирован с одним или более из типа активов, стоимости активов, скрытой в фиксации, и случайного числа, используемого для формирования фиксации. В некоторых реализациях, консенсусный узел определяет то, что каждый из множества активов ассоциирован с идентичным типом активов. В некоторых реализациях, первая фиксация, вторая фиксация и фиксация, которая скрывает стоимость активов, формируются на основе схемы фиксации, которая является гомоморфной.

[0089] В некоторых реализациях, третье случайное число шифруется на основе вероятностной HE-схемы посредством трактовки суммы транзакции в качестве случайного числа, и четвертое случайное число шифруется на основе вероятностной HE-схемы посредством трактовки сдачи в качестве случайного числа. В некоторых реализациях, первая фиксация и вторая фиксация формируются на основе схемы фиксации Педерсена, и вероятностная HE-схема представляет собой схему OU-шифрования.

[0090] В некоторых реализациях, ZKP содержит фиксацию Педерсена, которая скрывает пятое случайное число и шестое случайное число, шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа второго счета на основе схемы OU-шифрования, и шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа первого счета на основе схемы OU-шифрования.

[0091] На 604, консенсусный узел верифицирует цифровую подпись на основе открытого ключа первого узла.

[0092] На 606, консенсусный узел определяет то, что одно или более доказательств по диапазону доказывают то, что сумма транзакции и сдача превышают или равны нулю.

[0093] На 608, консенсусный узел определяет то, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи. В некоторых реализациях, определение того, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи, выполняется на основе гомоморфизма схемы фиксации.

[0094] На 610, консенсусный узел определяет, на основе ZKP, то, что транзакция является достоверной, посредством определения того, что первое случайное число равно третьему случайному числу, второе случайное число равно четвертому случайному числу, и сумма транзакции, скрытая в первой фиксации, равна сумме транзакции, зашифрованной посредством открытого ключа второго узла.

[0095] В некоторых реализациях, транзакция выполняется между счетом, ассоциированным с первым узлом, и счетом, ассоциированным со вторым узлом, и способ дополнительно содержит обновление, после определения того, что транзакция является достоверной, счета, ассоциированного с первым узлом, и счета, ассоциированного со вторым узлом, на основе суммы транзакции и сдачи. В некоторых реализациях, ZKP формируется и используется для определения того, что транзакция является достоверной, на основе свойств вероятностного HE. В некоторых реализациях, определение того, что транзакция является достоверной, выполняется на основе ZKP без взаимодействий между первым узлом и вторым узлом через часть за пределами сети цепочек блоков.

[0096] Фиг. 7 иллюстрирует примерный процесс 700, который может выполняться в

соответствии с реализациями описания изобретения. Для ясности представления, нижеприведенное описание, в общем, описывает способ 700 в контексте других чертежей в этом описании. Тем не менее, следует понимать, что примерный процесс 700 может выполняться, например, посредством любой системы, окружения, программного обеспечения и аппаратных средств либо комбинации систем, окружений, программного обеспечения и аппаратных средств, надлежащим образом. В некоторых реализациях, этапы примерного процесса 700 могут выполняться параллельно, в комбинации, циклически или в любом порядке.

[0097] На 702, консенсусный узел принимает данные транзакции, ассоциированные с транзакцией. В некоторых примерах, данные транзакции содержат данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, вычисленную на основе удержания суммы транзакции из полной стоимости множества активов, сумму транзакции и третье случайное число, оба из которых шифруются посредством открытого ключа второго узла на основе линейной детерминированной HE-схемы, сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе линейной детерминированной HE-схемы, одно или более доказательств по диапазону, ZKP и цифровую подпись, сформированную на основе закрытого ключа, соответствующего открытому ключу первого узла.

[0098] В некоторых реализациях, каждый из множества активов ассоциирован с одним или более из типа активов, стоимости активов, скрытой в фиксации, и случайного числа, используемого для формирования фиксации. В некоторых реализациях, консенсусный узел определяет то, что каждый из множества активов ассоциирован с идентичным типом активов. В некоторых реализациях, первая фиксация, вторая фиксация и фиксация, которая скрывает стоимость активов, формируются на основе схемы фиксации, которая является гомоморфной.

[0099] В некоторых реализациях, линейная детерминированная HE-схема извлекается из вероятностной HE-схемы на основе изменения случайного числа, ассоциированного с вероятностной HE-схемой, на фиксированное число.

[00100] В некоторых реализациях, ZKP содержит фиксацию, которая скрывает пятое случайное число и шестое случайное число, шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа второго счета на основе линейной детерминированной HE-схемы, и шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа первого счета на основе линейной детерминированной HE-схемы.

[00101] На 704, консенсусный узел верифицирует цифровую подпись на основе открытого ключа первого узла.

[00102] На 706, консенсусный узел определяет то, что одно или более доказательств по диапазону доказывают то, что сумма транзакции и сдача превышают или равны нулю.

[00103] На 708, консенсусный узел определяет то, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи. В некоторых реализациях, определение того, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи, выполняется на основе гомоморфизма схемы фиксации.

[00104] На 710, консенсусный узел определяет, на основе ZKP, то, что транзакция является достоверной, посредством определения того, что первое случайное число равно третьему случайному числу, второе случайное число равно четвертому случайному

числу, и сумма транзакции, скрытая в первой фиксации, равна сумме транзакции, зашифрованной посредством открытого ключа второго узла.

[00105] В некоторых реализациях, транзакция выполняется между счетом, ассоциированным с первым узлом, и счетом, ассоциированным со вторым узлом, и способ дополнительно содержит обновление, после определения того, что транзакция является достоверной, счета, ассоциированного с первым узлом, и счета, ассоциированного со вторым узлом, на основе суммы транзакции и сдачи. В некоторых реализациях, ZKP формируется и используется для определения того, что транзакция является достоверной, на основе свойств линейного детерминированного НЕ. В некоторых реализациях, определение того, что транзакция является достоверной, выполняется на основе ZKP без взаимодействий между первым узлом и вторым узлом через часть за пределами сети цепочек блоков.

[00106] Фиг. 8 иллюстрирует пример узла 800 цепочки блоков, который может выполнять процесс в соответствии с реализациями описания изобретения. На высоком уровне, узел 800 цепочки блоков включает в себя приемный блок 802, блок 804 верификации, первый блок 806 определения, второй блок 808 определения и третий блок 810 определения.

[00107] В некоторых реализациях, приемный блок 802 выполнен с возможностью принимать данные транзакции, ассоциированные с транзакцией. В некоторых примерах, данные транзакции содержат данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, вычисленную на основе удержания суммы транзакции из полной стоимости множества активов, сумму транзакции и третье случайное число, оба из которых шифруются посредством открытого ключа второго узла на основе вероятностной НЕ-схемы, сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе вероятностной НЕ-схемы, одно или более доказательств по диапазону, ZKP и цифровую подпись, сформированную на основе закрытого ключа, соответствующего открытому ключу первого узла.

[00108] В некоторых реализациях, приемный блок 802 выполнен с возможностью принимать данные транзакции, ассоциированные с транзакцией, причем данные транзакции содержат: данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, вычисленную на основе удержания суммы транзакции из полной стоимости множества активов, сумму транзакции и третье случайное число, оба из которых шифруются посредством открытого ключа второго узла на основе линейной детерминированной НЕ-схемы, сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе линейной детерминированной НЕ-схемы, одно или более доказательств по диапазону, ZKP и цифровую подпись, сформированную на основе закрытого ключа, соответствующего открытому ключу первого узла.

[00109] В некоторых реализациях, каждый из множества активов ассоциирован с одним или более из типа активов, стоимости активов, скрытой в фиксации, и случайного числа, используемого для формирования фиксации. В некоторых реализациях, узел 800 цепочки блоков определяет то, что каждый из множества активов ассоциирован с идентичным типом активов. В некоторых реализациях, первая фиксация, вторая фиксация и фиксация, которая скрывает стоимость активов, формируются на основе схемы фиксации, которая является гомоморфной. В некоторых реализациях, линейная

детерминированная HE-схема извлекается из вероятностной HE-схемы на основе изменения случайного числа, ассоциированного с вероятностной HE-схемой, на фиксированное число.

[00110] В некоторых реализациях, третье случайное число шифруется на основе вероятностной HE-схемы посредством трактовки суммы транзакции в качестве случайного числа, и четвертое случайное число шифруется на основе вероятностной HE-схемы посредством трактовки сдачи в качестве случайного числа. В некоторых реализациях, первая фиксация и вторая фиксация формируются на основе схемы фиксации Педерсена, и вероятностная HE-схема представляет собой схему OU-шифрования.

[00111] В некоторых реализациях, ZKP содержит фиксацию Педерсена, которая скрывает пятое случайное число и шестое случайное число, шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа второго счета на основе схемы OU-шифрования, и шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа первого счета на основе схемы OU-шифрования. В некоторых реализациях, ZKP содержит фиксацию, которая скрывает пятое случайное число и шестое случайное число, шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа второго счета на основе линейной детерминированной HE-схемы, и шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа первого счета на основе линейной детерминированной HE-схемы.

[00112] Блок 804 верификации выполнен с возможностью верифицировать цифровую подпись на основе открытого ключа первого узла.

[00113] Первый блок 806 определения выполнен с возможностью определять то, что одно или более доказательств по диапазону доказывают то, что сумма транзакции и сдача больше или равны нулю.

[00114] Второй блок 808 определения выполнен с возможностью определять то, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи. В некоторых реализациях, определение того, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи, выполняется на основе гомоморфизма схемы фиксации.

[00115] Третий блок 810 определения выполнен с возможностью определять, на основе ZKP, то, что транзакция является достоверной, посредством определения того, что первое случайное число равно третьему случайному числу, второе случайное число равно четвертому случайному числу, и сумма транзакции, скрытая в первой фиксации, равна сумме транзакции, зашифрованной посредством открытого ключа второго узла.

[00116] В некоторых реализациях, транзакция выполняется между счетом, ассоциированным с первым узлом, и счетом, ассоциированным со вторым узлом, и узел 800 цепочки блоков может включать в себя блок обновления, выполненный с возможностью обновлять, после того, как третий блок 810 определения определяет то, что транзакция является достоверной, счет, ассоциированный с первым узлом, и счет, ассоциированный со вторым узлом, на основе суммы транзакции и сдачи. В некоторых реализациях, ZKP формируется и используется для определения того, что транзакция является достоверной, на основе свойств вероятностного HE. В некоторых реализациях, ZKP формируется и используется для определения того, что транзакция является достоверной, на основе свойств линейного детерминированного HE. В некоторых реализациях, определение того, что транзакция является достоверной, выполняется на

основе ZKP без взаимодействий между первым узлом и вторым узлом через часть за пределами сети цепочек блоков.

[00117] Реализации предмета изобретения, описанного в этом подробном описании, могут реализовываться таким образом, чтобы реализовывать конкретные преимущества или технические эффекты. Например, реализации описания изобретения разрешают балансу счета и сумме транзакции узлов цепочки блоков быть закрытыми во время транзакций. Получатель перевода денежных средств не должен обязательно подтверждать транзакцию или использовать случайное число для того, чтобы верифицировать фиксацию, проверка достоверности транзакций может быть неинтерактивной. Узел цепочки блоков может проверять достоверность транзакции на основе HE и схем фиксации, чтобы обеспечивать возможность доказательства с нулевой передачей знаний.

[00118] Описанная технология разрешает повышение безопасности счетов/данных различного мобильного вычислительного устройства. Баланс счетов и суммы транзакций могут шифроваться на основе HE и скрываться посредством схем фиксации. В связи с этим, консенсусный узел может обновлять баланс счетов в реестре после транзакции на основе свойств HE без раскрытия фактического баланса счета для счета. Поскольку случайное число не должно обязательно отправляться получателю, чтобы подтверждать транзакцию, риск утечки данных может уменьшаться, и меньший объем вычислительных ресурсов и ресурсов запоминающего устройства должен использоваться для того, чтобы управлять случайным числом.

[00119] Реализации и операции, описанные в этом подробном описании, могут реализовываться в цифровой электронной схеме или в компьютерном программном обеспечении, микропрограммном обеспечении или аппаратных средствах, включающих в себя структуры, раскрытые в этом подробном описании, либо в комбинациях одного или более из означенного. Операции могут реализовываться как операции, выполняемые посредством оборудования обработки данных для данных, сохраненных на одном или более машиночитаемых устройств хранения данных или принимаемых из других источников. Оборудование обработки данных, компьютер или вычислительное устройство может охватывать оборудование, устройства и машины для обработки данных, включающие в себя в качестве примера программируемый процессор, компьютер, внутрикристальную систему либо несколько из вышеприведенного, либо комбинации вышеприведенного. Оборудование может включать в себя логическую схему специального назначения, например, центральный процессор (CPU), программируемую пользователем вентильную матрицу (FPGA) или специализированную интегральную схему (ASIC). Оборудование также может включать в себя код, который создает окружение выполнения для рассматриваемой компьютерной программы, например, код, который составляет микропрограммное обеспечение процессора, стек протоколов, систему управления базами данных, операционную систему (например, операционную систему или комбинацию операционных систем), кросс-платформенное окружение выполнения, виртуальную машину либо комбинацию одного или более из означенного. Оборудование и окружение выполнения могут реализовывать всевозможные инфраструктуры вычислительных моделей, такие как веб-услуги, распределенные вычислительные и сетевые параллельные вычислительные инфраструктуры.

[00120] Компьютерная программа (также известная, например, в качестве программы, программного обеспечения, приложения, программного модуля, программного блока, сценария или кода) может быть написана на любой форме языка программирования,

включающей в себя компилированные или интерпретируемые языки, декларативные или процедурные языки, и она может развертываться в любой форме, в том числе в качестве автономной программы или в качестве модуля, компонента, вложенной процедуры, объекта либо другого блока, подходящего для использования в вычислительном окружении. Программа может сохраняться в части файла, который хранит другие программы или данные (например, один или более сценариев, сохраненных в документе на языке разметки), в одном файле, выделенном для рассматриваемой программы, либо в нескольких координированных файлах (например, в файлах, которые сохраняют один или более модулей, подпрограмм или частей кода). Компьютерная программа может выполняться на одном компьютере или на нескольких компьютерах, которые расположены на одном веб-узле или распределены по нескольким веб-узлам и взаимно соединяются посредством сети связи.

[00121] Процессоры для выполнения компьютерной программы включают в себя, в качестве примера, микропроцессоры общего и специального назначения и любые один или более процессоров любого вида цифрового компьютера. В общем, процессор принимает инструкции и данные из постоянного запоминающего устройства или оперативного запоминающего устройства, или из того и из другого. Существенные элементы компьютера представляют собой процессор для выполнения действий в соответствии с инструкциями и одно или более запоминающих устройств для сохранения инструкций и данных. Обычно, компьютер также должен включать в себя или функционально соединяться с возможностью принимать данные или передавать данные либо выполнять и то, и другое из/в одно или более устройств хранения данных большой емкости для сохранения данных. Компьютер может встраиваться в другое устройство, например, в мобильное устройство, персональное цифровое устройство (PDA), игровую приставку, приемное устройство на основе глобальной системы позиционирования (GPS) или портативное устройство хранения данных. Устройства, подходящие для сохранения компьютерных программных инструкций и данных, включают в себя энергонезависимое запоминающее устройство, носители и запоминающие устройства, включающие в себя, в качестве примера, полупроводниковые запоминающие устройства, магнитные диски и магнитооптические диски. Процессор и запоминающее устройство могут дополняться посредством или включаться в логическую схему специального назначения.

[00122] Мобильные устройства могут включать в себя переносные телефоны, абонентские устройства (UE), мобильные телефоны (например, смартфоны), планшетные компьютеры, носимые устройства (например, интеллектуальные часы и интеллектуальные очки), имплантируемые устройства в человеческом теле (например, биодатчики, кохлеарные имплантаты) либо другие типы мобильных устройств. Мобильные устройства могут обмениваться данными в беспроводном режиме (например, с использованием радиочастотных (RF) сигналов) с различными сетями связи (описаны ниже). Мобильные устройства могут включать в себя датчики для определения характеристик текущего окружения мобильного устройства. Датчики могут включать в себя камеры, микрофоны, бесконтактные датчики, GPS-датчики, датчики движения, акселерометры, датчики окружающего света, датчики содержания влаги, гироскопы, компасы, барометры, датчики отпечатков пальцев, системы распознавания лиц, RF-датчики (например, Wi-Fi- и сотовые радиомодули), тепловые датчики или другие типы датчиков. Например, камеры могут включать в себя обращенную по ходу движения или против движения камеру с подвижными или неподвижными линзами, флэш-памятью, датчиком изображений и процессором

изображений. Камера может представлять собой мегапиксельную камеру, допускающую захват деталей для распознавания лиц и/или радужной оболочки глаз. Камера наряду с процессором данных и аутентификационной информацией, сохраненной в запоминающем устройстве или доступной удаленно, может формировать систему распознавания лиц. Система распознавания лиц либо один или более датчиков, например, микрофонов, датчиков движения, акселерометров, GPS-датчиков или RF-датчиков, могут использоваться для аутентификации пользователя.

[00123] Чтобы предоставлять взаимодействие с пользователем, реализации могут реализовываться на компьютере, имеющем устройство отображения и устройство ввода, например, жидкокристаллический дисплей (ЖК-дисплей) или дисплей на органических светоизлучающих диодах (OLED)/в стиле виртуальной реальности (VR) /в стиле дополненной реальности (AR) для отображения информации пользователю и сенсорный экран, клавиатуру и указательное устройство, посредством которых пользователь может предоставлять ввод в компьютер. Другие виды устройств также могут использоваться для того, чтобы предоставлять взаимодействие с пользователем; например, обратная связь, предоставленная пользователю, может представлять собой любую форму сенсорной обратной связи, например, визуальную обратную связь, акустическую обратную связь или тактильную обратную связь; и ввод от пользователя может приниматься в любой форме, включающей в себя акустический, речевой или тактильный ввод. Помимо этого, компьютер может взаимодействовать с пользователем посредством отправки документов и приема документов из устройства, которое используется пользователем; например, посредством отправки веб-страниц в веб-браузер на клиентском устройстве пользователя в ответ на запросы, принимаемые из веб-браузера.

[00124] Реализации могут реализовываться с использованием вычислительных устройств, взаимно соединенных посредством любой формы или среды для проводной или беспроводной цифровой передачи данных (либо комбинации вышеозначенного), например, сети связи. Примеры взаимно соединенных устройств представляют собой клиент и сервер, в общем, удаленные друг от друга, которые типично взаимодействуют через сеть связи. Клиент, например, мобильное устройство, может выполнять транзакции непосредственно, с сервером или через сервер, например, выполнять транзакции покупки, продажи, оплаты, выдачи, отправки или ссуды либо авторизовать их. Такие транзакции могут выполняться в реальном времени таким образом, что действие и ответ являются близкими по времени; например, человек воспринимает действие и ответ как возникающие практически одновременно, разность времен для ответа после действия человека составляет меньше 1 миллисекунды (мс) или меньше 1 секунды (с), либо ответ осуществляется без намеренной задержки с учетом ограничений обработки системы.

[00125] Примеры сетей связи включают в себя локальную вычислительную сеть (LAN), сеть радиодоступа (RAN), общегородскую вычислительную сеть (MAN) и глобальную вычислительную сеть (WAN). Сеть связи может включать в себя все или часть из Интернета, другой сети связи либо комбинации сетей связи. Информация может передаваться по сети связи согласно различным протоколам и стандартам, включающим в себя стандарт долгосрочного развития (LTE), 5G, IEEE 802, Интернет-протокол (IP) либо другие протоколы или комбинации протоколов. Сеть связи может передавать голосовые, видео-, биометрические данные или аутентификационные данные или другую информацию между соединенными вычислительными устройствами.

[00126] Признаки, описанные в качестве отдельных реализаций, могут реализовываться, в комбинации, в одной реализации, в то время как признаки, описанные

в качестве одной реализации, могут реализовываться в нескольких реализациях, отдельно или в любой подходящей субкомбинации. Операции, описанные и заявленные в конкретном порядке, не должны пониматься ни как требующие этого конкретного порядка, ни как то, что все проиллюстрированные операции должны выполняться (некоторые операции могут быть необязательными). Надлежащим образом, могут выполняться многозадачность или параллельная обработка (или комбинация многозадачности и параллельной обработки).

(57) Формула изобретения

1. Машинореализованный способ, осуществляемый посредством консенсусного узла для проверки достоверности транзакции между первым узлом и вторым узлом в сети цепочек блоков, при этом способ содержит этапы, на которых:

- принимают данные транзакции, ассоциированные с транзакцией, причем данные транзакции содержат: данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, вычисленную на основе удержания суммы транзакции из полной стоимости множества активов, сумму транзакции и третье случайное число, оба из которых шифруются посредством открытого ключа второго узла на основе линейной детерминированной схемы гомоморфного шифрования (HE), сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе линейной детерминированной HE-схемы, одно или более доказательств по диапазону, доказательство с нулевой передачей знаний (ZKP) и цифровую подпись, сформированную на основе закрытого ключа, соответствующего открытому ключу первого узла;

- верифицируют цифровую подпись на основе открытого ключа первого узла;

- определяют, что значение одного или более доказательств по диапазону, которое ассоциировано с суммой транзакции, и значение другого из одного или более доказательств по диапазону, которое ассоциировано со сдачей, указывают, что сумма транзакции и сдача каждая превышают или равны нулю;

- определяют то, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи; и

- определяют, на основе ZKP, то, что транзакция является достоверной, посредством определения того, что первое случайное число равно третьему случайному числу, второе случайное число равно четвертому случайному числу, и сумма транзакции, скрытая в первой фиксации, равна сумме транзакции, зашифрованной посредством открытого ключа второго узла.

2. Машинореализованный способ по п. 1, в котором транзакция выполняется между счетом, ассоциированным с первым узлом, и счетом, ассоциированным со вторым узлом, и способ дополнительно содержит этап, на котором обновляют, после определения того, что транзакция является достоверной, счет, ассоциированный с первым узлом, и счет, ассоциированный со вторым узлом, на основе суммы транзакции и сдачи.

3. Машинореализованный способ по п. 1, в котором каждый из множества активов ассоциирован с одним или более из типа активов, стоимости активов, скрытой в фиксации, и случайного числа, используемого для формирования фиксации.

4. Машинореализованный способ по п. 3, дополнительно содержащий этап, на котором определяют то, что каждый из множества активов ассоциирован с идентичным типом активов.

5. Машинореализованный способ по п. 3, в котором первая фиксация, вторая фиксация и фиксация, которая скрывает стоимость активов, формируются на основе схемы фиксации, которая является гомоморфной, при этом определение того, что полная стоимость множества активов равна суммарной величине суммы транзакции и сдачи, выполняется на основе гомоморфизма схемы фиксации.

6. Машинореализованный способ по п. 1, в котором линейная детерминированная НЕ-схема извлекается из вероятностной НЕ-схемы на основе изменения случайного числа, ассоциированного с вероятностной НЕ-схемой, на фиксированное число.

7. Машинореализованный способ по п. 1, в котором ZKP содержит фиксацию, которая скрывает пятое случайное число и шестое случайное число, шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа второго счета на основе линейной детерминированной НЕ-схемы, и шифрованный текст пятого случайного числа и шестого случайного числа, зашифрованный посредством открытого ключа первого счета на основе линейной детерминированной НЕ-схемы.

8. Машинореализованный способ по п. 1, в котором ZKP формируется и используется для определения того, что транзакция является достоверной, на основе свойств линейного детерминированного НЕ.

9. Машинореализованный способ по п. 1, в котором определение того, что транзакция является достоверной, выполняется на основе ZKP без взаимодействий между первым узлом и вторым узлом через часть за пределами сети цепочек блоков.

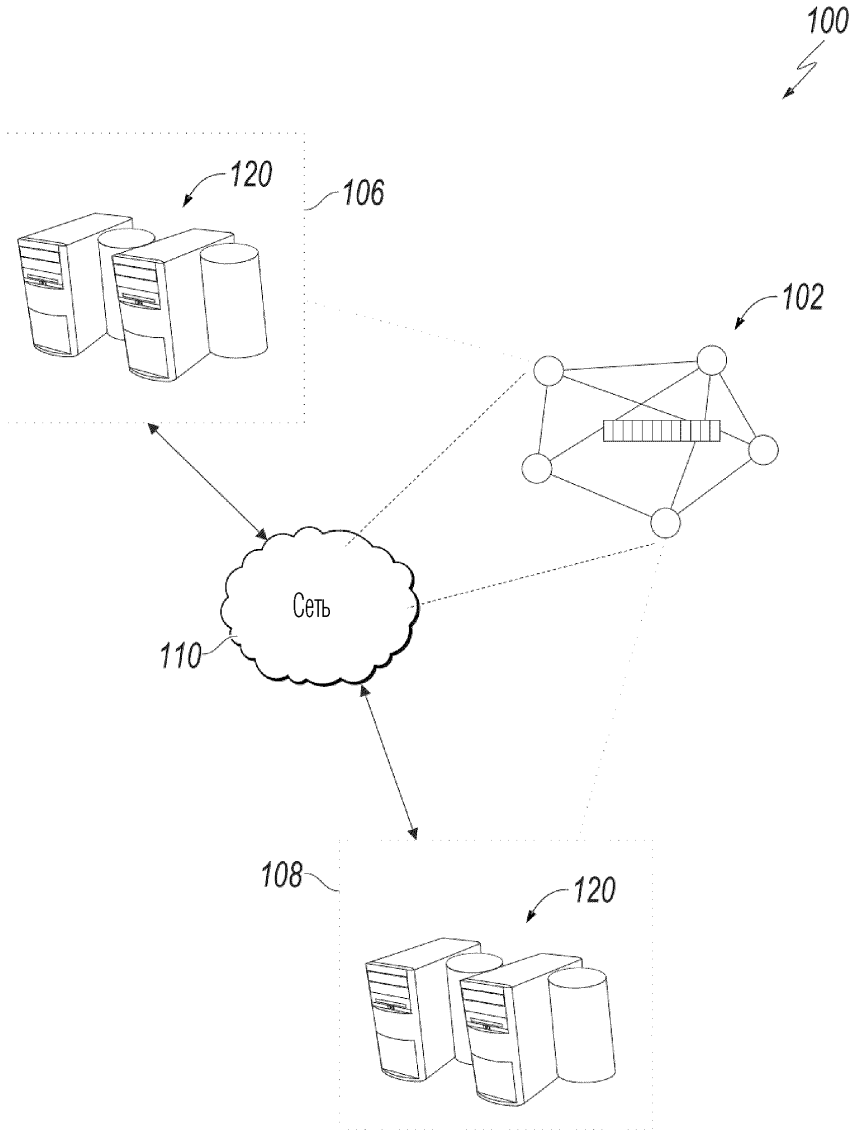
10. Энергонезависимый машиночитаемый носитель хранения данных, соединенный с одним или более компьютерами и сконфигурированный с инструкциями, выполняемыми посредством одного или более компьютеров с возможностью выполнять операции в соответствии со способом по одному или более из пп. 1-9.

11. Система для проверки достоверности транзакции между первым узлом и вторым узлом в сети цепочек блоков, содержащая:

- один или более компьютеров; и

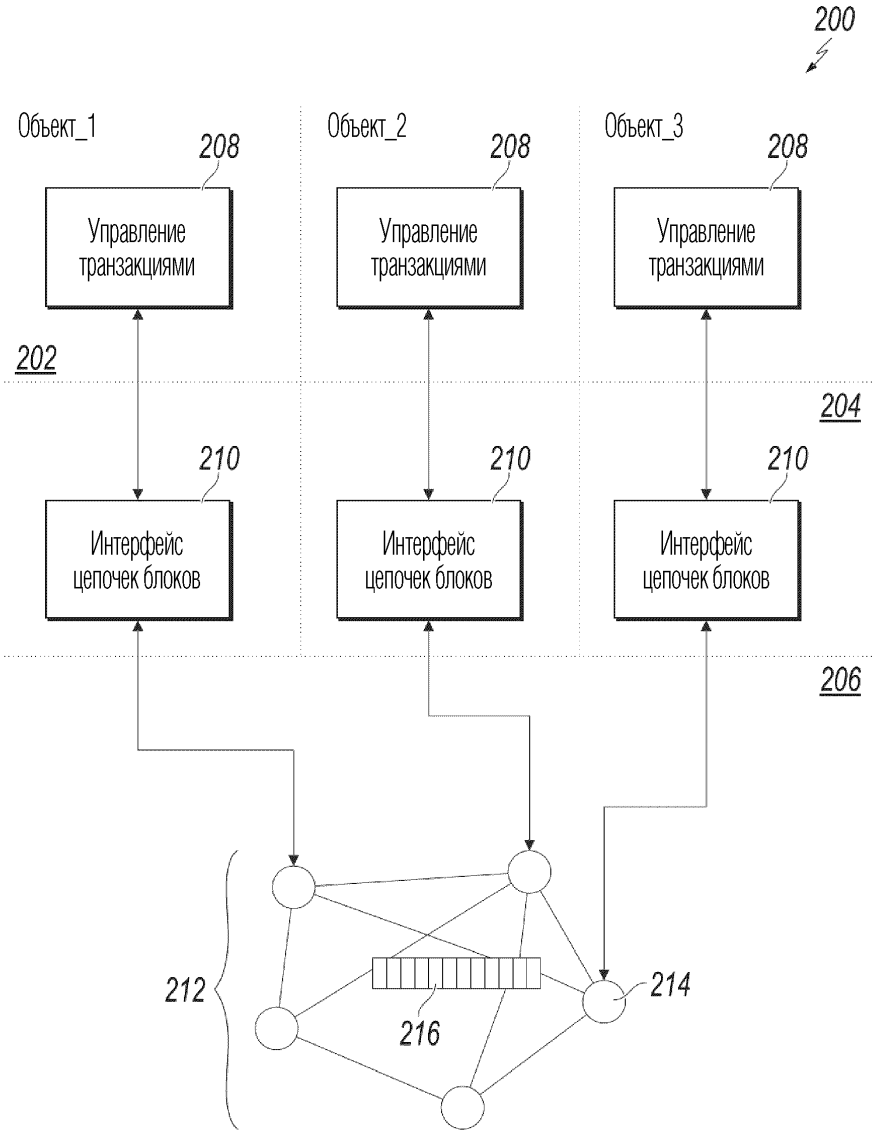
- одно или более машиночитаемых запоминающих устройств, соединенных с одним или более компьютерами и сконфигурированных с инструкциями, выполняемыми посредством одного или более компьютеров с возможностью выполнять операции в соответствии со способом по одному или более из пп. 1-9.

1



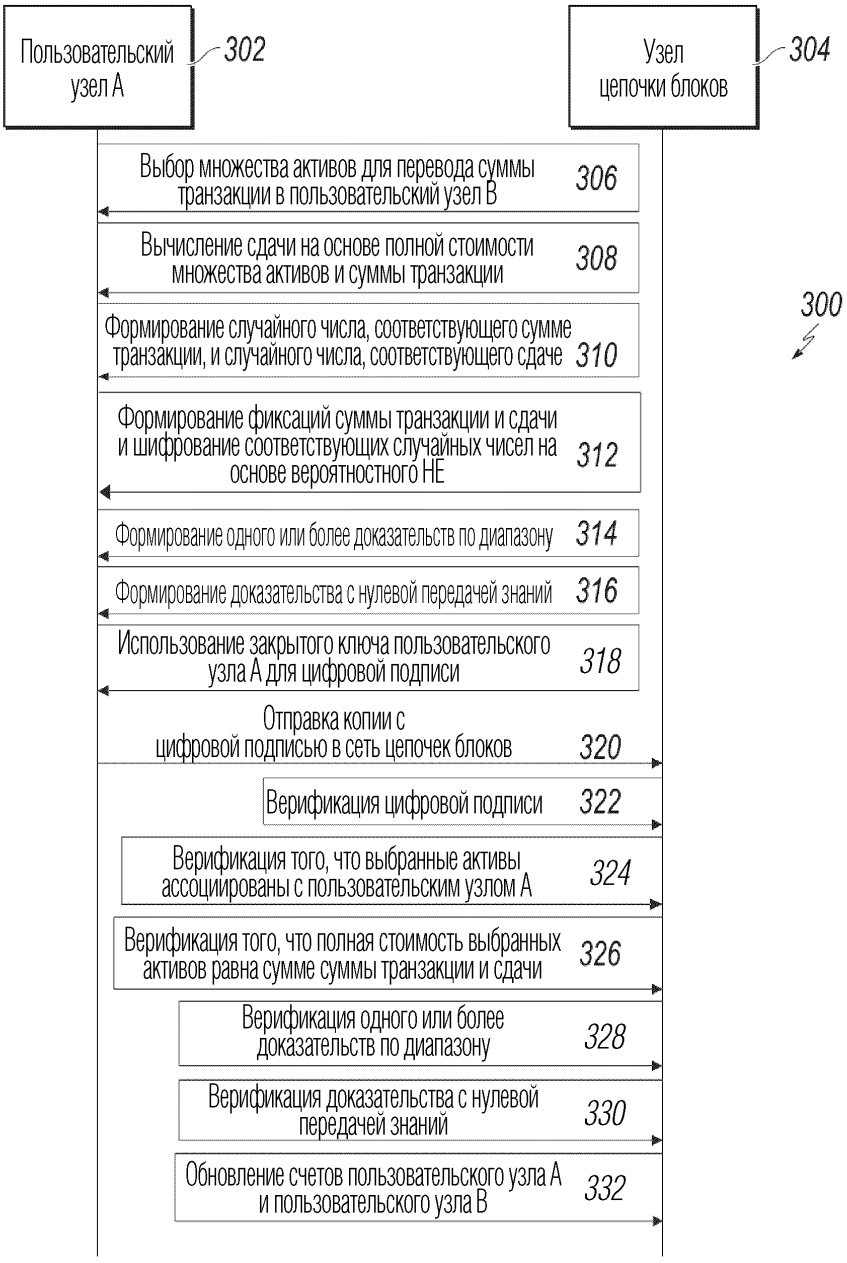
ФИГ. 1

2


200
Объект_1
208
Управление транзакциями
Объект_2
208
Управление транзакциями
Объект_3
208
Управление транзакциями
202
204
210
Интерфейс цепочек блоков
210
Интерфейс цепочек блоков
210
Интерфейс цепочек блоков
206
212
214
216

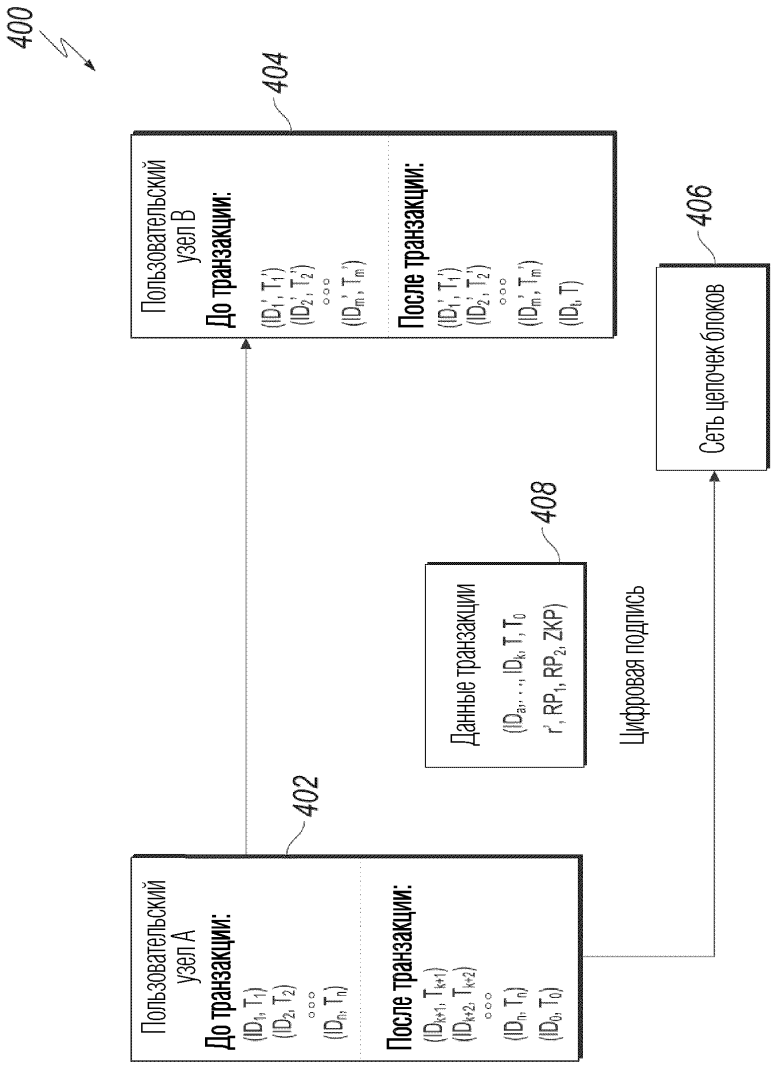
ФИГ. 2

3


Пользовательский узел A
302
Узел цепочки блоков
304
Выбор множества активов для перевода суммы транзакции в пользовательский узел B
306
Вычисление сдачи на основе полной стоимости множества активов и суммы транзакции
308
Формирование случайного числа, соответствующего сумме транзакции, и случайного числа, соответствующего сдаче
310
Формирование фиксаций суммы транзакции и сдачи и шифрование соответствующих случайных чисел на основе вероятностного HE
312
Формирование одного или более доказательств по диапазону
314
Формирование доказательства с нулевой передачей знаний
316
Использование закрытого ключа пользовательского узла A для цифровой подписи
318
Отправка копии с цифровой подписью в сеть цепочек блоков
320
Верификация цифровой подписи
322
Верификация того, что выбранные активы ассоциированы с пользовательским узлом A
324
Верификация того, что полная стоимость выбранных активов равна сумме суммы транзакции и сдачи
326
Верификация одного или более доказательств по диапазону
328
Верификация доказательства с нулевой передачей знаний
330
Обновление счетов пользовательского узла A и пользовательского узла B
332
300

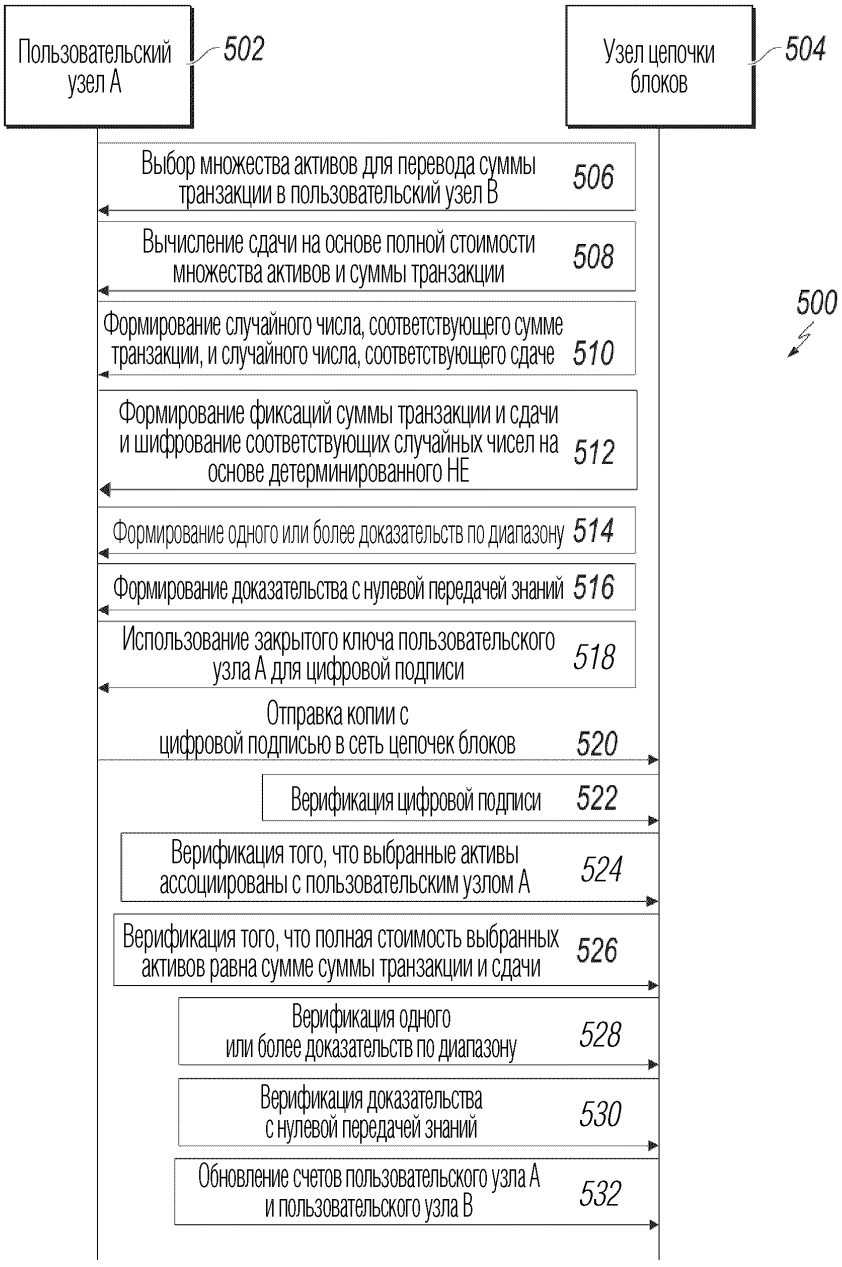
ФИГ. 3

4


400
404
Пользовательский узел B
До транзакции:
(ID1, T1')
(ID2, T2')
...
(IDm, Tm')
После транзакции:
(ID1', T1')
(ID2', T2')
...
(IDm', Tm')
(IDb, T)
406
Сеть цепочек блоков
408
Данные транзакции
(IDa1, ..., IDak, T, T0
r', RP1, RP2, ZKP)
Цифровая подпись
402
Пользовательский узел A
До транзакции:
(ID1, T1)
(ID2, T2)
...
(IDn, Tn)
После транзакции:
(IDk+1, Tk+1)
(IDk+2, Tk+2)
...
(IDn, Tn)
(IDb, T0)

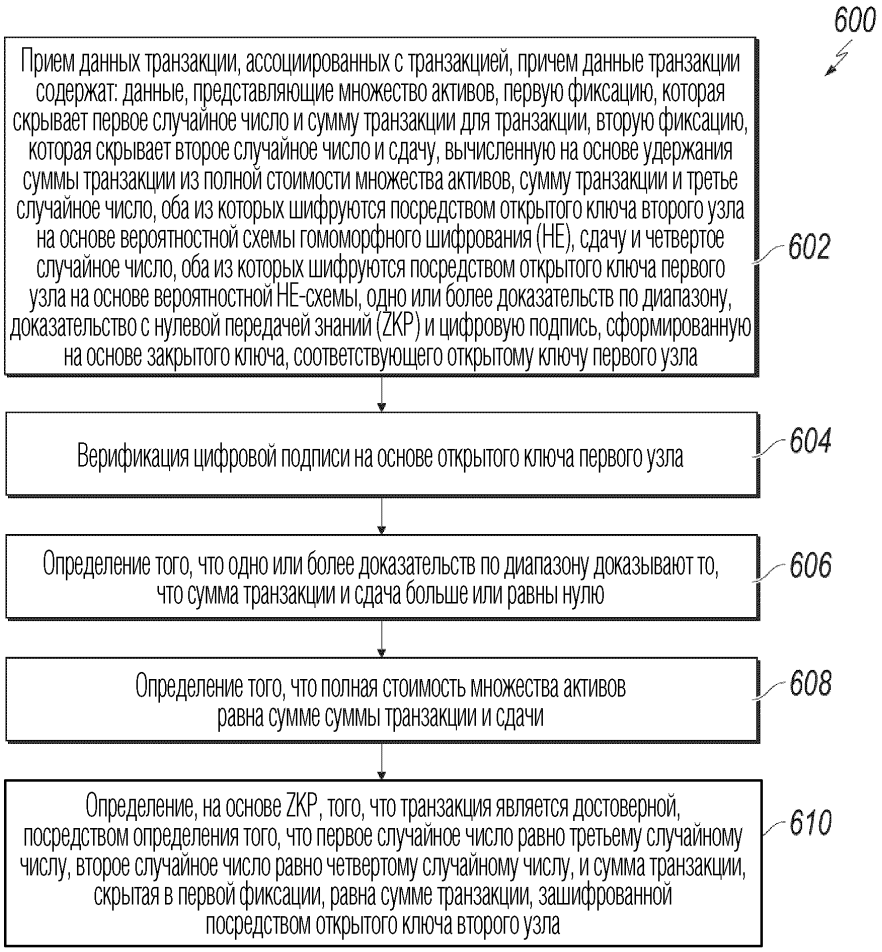
ФИГ. 4

5


Пользовательский узел A
502
Узел цепочки блоков
504
500
Выбор множества активов для перевода суммы транзакции в пользовательский узел B
506
Вычисление сдачи на основе полной стоимости множества активов и суммы транзакции
508
Формирование случайного числа, соответствующего сумме транзакции, и случайного числа, соответствующего сдаче
510
Формирование фиксаций суммы транзакции и сдачи и шифрование соответствующих случайных чисел на основе детерминированного HE
512
Формирование одного или более доказательств по диапазону
514
Формирование доказательства с нулевой передачей знаний
516
Использование закрытого ключа пользовательского узла A для цифровой подписи
518
Отправка копии с цифровой подписью в сеть цепочек блоков
520
Верификация цифровой подписи
522
Верификация того, что выбранные активы ассоциированы с пользовательским узлом A
524
Верификация того, что полная стоимость выбранных активов равна сумме суммы транзакции и сдачи
526
Верификация одного или более доказательств по диапазону
528
Верификация доказательства с нулевой передачей знаний
530
Обновление счетов пользовательского узла A и пользовательского узла B
532

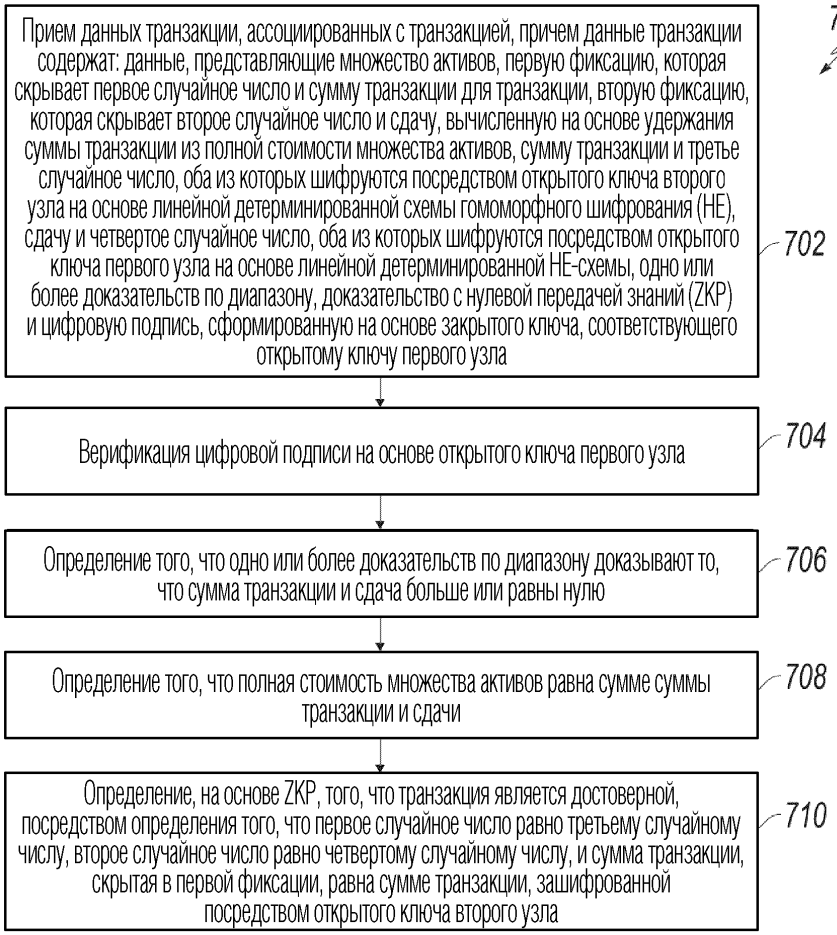
ФИГ. 5

6


600
Прием данных транзакции, ассоциированных с транзакцией, причем данные транзакции содержат: данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, вычисленную на основе удержания суммы транзакции из полной стоимости множества активов, сумму транзакции и третье случайное число, оба из которых шифруются посредством открытого ключа второго узла на основе вероятностной схемы гомоморфного шифрования (HE), сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе вероятностной HE-схемы, одно или более доказательств по диапазону, доказательство с нулевой передачей знаний (ZKP) и цифровую подпись, сформированную на основе закрытого ключа, соответствующего открытому ключу первого узла
602
Верификация цифровой подписи на основе открытого ключа первого узла
604
Определение того, что одно или более доказательств по диапазону доказывают то, что сумма транзакции и сдача больше или равны нулю
606
Определение того, что полная стоимость множества активов равна сумме суммы транзакции и сдачи
608
Определение, на основе ZKP, того, что транзакция является достоверной, посредством определения того, что первое случайное число равно третьему случайному числу, второе случайное число равно четвертому случайному числу, и сумма транзакции, скрытая в первой фиксации, равна сумме транзакции, зашифрованной посредством открытого ключа второго узла
610

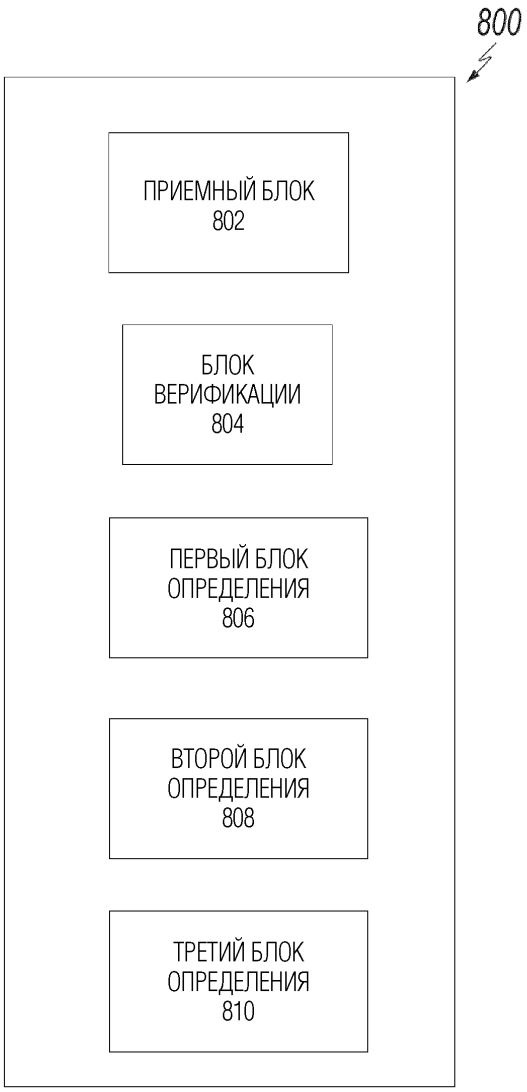
ФИГ. 6

7


700
Прием данных транзакции, ассоциированных с транзакцией, причем данные транзакции содержат: данные, представляющие множество активов, первую фиксацию, которая скрывает первое случайное число и сумму транзакции для транзакции, вторую фиксацию, которая скрывает второе случайное число и сдачу, вычисленную на основе удержания суммы транзакции из полной стоимости множества активов, сумму транзакции и третье случайное число, оба из которых шифруются посредством открытого ключа второго узла на основе линейной детерминированной схемы гомоморфного шифрования (HE), сдачу и четвертое случайное число, оба из которых шифруются посредством открытого ключа первого узла на основе линейной детерминированной HE-схемы, одно или более доказательств по диапазону, доказательство с нулевой передачей знаний (ZKP) и цифровую подпись, сформированную на основе закрытого ключа, соответствующего открытому ключу первого узла
702
Верификация цифровой подписи на основе открытого ключа первого узла
704
Определение того, что одно или более доказательств по диапазону доказывают то, что сумма транзакции и сдача больше или равны нулю
706
Определение того, что полная стоимость множества активов равна сумме суммы транзакции и сдачи
708
Определение, на основе ZKP, того, что транзакция является достоверной, посредством определения того, что первое случайное число равно третьему случайному числу, второе случайное число равно четвертому случайному числу, и сумма транзакции, скрытая в первой фиксации, равна сумме транзакции, зашифрованной посредством открытого ключа второго узла
710

ФИГ. 7

8


800
ПРИЕМНЫЙ БЛОК
802
БЛОК
ВЕРИФИКАЦИИ
804
ПЕРВЫЙ БЛОК
ОПРЕДЕЛЕНИЯ
806
ВТОРОЙ БЛОК
ОПРЕДЕЛЕНИЯ
808
ТРЕТИЙ БЛОК
ОПРЕДЕЛЕНИЯ
810

ФИГ. 8