(19) Евразийское патентное ведомство

(11) 038684 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.10.04

(21) Номер заявки
201991995

(22) Дата подачи заявки
2017.11.22

(51) Int. Cl. ***G06Q 20/06*** (2012.01)
G06Q 20/40 (2012.01)

(54) УСОВЕРШЕНСТВОВАННЫЕ СПОСОБЫ, СИСТЕМЫ И УСТРОЙСТВА ДЛЯ РЕГИСТРАЦИИ ИНФОРМАЦИИ В БАЗЕ ДАННЫХ

(31) **17159825.3; 17172713.4**
(32) **2017.03.08; 2017.05.24**
(33) **EP**
(43) **2020.01.31**
(86) **PCT/EP2017/080043**
(87) **WO 2018/162099 2018.09.13**

(71)(73) Заявитель и патентовладелец:
СИКПА ХОЛДИНГ СА (CH)

(72) Изобретатель:
Тевоз Филипп (CH)

(74) Представитель:
Рыбина Н.А., Рыбин В.Н. (RU)

(56) WO-A1-2016170538
DE-A1-102014017710
US-A1-2012089519
Joseph Poon ET AL.: "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", 14 January 2016 (2016-01-14), XP055358006, Retrieved from the Internet: URL:https://lightning.network/lightning-network-paper.pdf, the whole document
Pedro Franco: "Understanding Bitcoin: Cryptography, Engineering and Economics", In: "Understanding Bitcoin: Cryptography, Engineering and Economics", 24 November 2014 (2014-11-24), Wiley, XP055393688, ISBN: 978-1-119-01916-9, pages ToC,Ch01-Ch02,Ch05-Ch07,Ch12-, the whole document

(57) Предусмотрены способ и система регистрации в базе данных транзакции между двумя сторонами и получения разрешения от третьей стороны на осуществление действия в отношении транзакции. Способ включает этап создания (s2) записи транзакции, этапы электронного подписывания (s4, s12, s18, s26) записи транзакции, этапы регистрации (s6, s14, s20, s28) записи транзакции в базе данных, этапы выдачи уведомления (s8, s16, s22) о регистрации записи транзакции в базе данных, этапы верификации (s10, s24) записи транзакции третьей стороной и этап получения разрешения (s30) от третьей стороны на осуществление действия на основе информации о содержимом транзакции.

038684 B1

038684 B1

Область техники

Изобретение относится к области прикладной информатики. В частности, изобретение относится к регистрации, т.е. записи, информации в компьютеризированной базе данных.

Предпосылки изобретения

Технология блокчейна используется в качестве основного компонента ныне известной цифровой валюты биткоин. В системе биткоинов блокчейн служит публичным реестром для всех транзакций (см. Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." (2008), документ извлечен 2 марта 2017 г. из сайта https://bitcoin.org/bitcoin.pdf).

Технология блокчейна вдохновила на исследования в прикладной информатике, особенно в областях баз данных, криптографии и компьютерных сетей. Некоторые из этих исследовательских мероприятий были сосредоточены на решении различных технических проблем, связанных с внедрением надежных, безопасных и эффективных компьютеризованных способов, систем и устройств для регистрации, т.е. записи, транзакций в компьютеризированной базе данных.

Краткое описание изобретения

Для решения или, по меньшей мере, частичного решения вышеупомянутых задач в независимых пунктах формулы изобретения определены способы, системы и электронные устройства согласно настоящему изобретению. В зависимых пунктах формулы изобретения определены конкретные варианты осуществления.

В одном варианте осуществления предусмотрен способ регистрации в базе данных транзакции между первой стороной, далее называемой как "Алиса", и второй стороной, далее называемой как "Боб", и получения разрешения от третьей стороны, далее называемой как "Кэрол", на осуществление действия в отношении транзакции. Каждая из сторон Алиса, Боб и Кэрол имеет электронное устройство, выполненное с возможностью осуществления связи с базой данных посредством сети связи и выполненное с возможностью электронного подписывания данных, подлежащих отправке посредством сети связи. Способ включает следующие этапы.

Электронное устройство Алисы обеспечивает создание записи, далее называемой как "запись транзакции". Запись транзакции включает: (i) идентификатор, далее называемый как "идентификатор транзакции", для идентификации транзакции, (ii) идентификатор для идентификации Алисы, (iii) идентификатор для идентификации Боба, и (iv) информацию, далее называемую как "информация о содержимом транзакции", относящуюся по меньшей мере к одному из: типа транзакции и ценности, которую, как полагают, имеет транзакция. Электронное устройство Алисы затем электронно подписывает запись транзакции. Полученная в результате запись транзакции далее называется как "TR_{kA}". TR_{kA} затем регистрируют в базе данных.

Электронное устройство Кэрол затем получает уведомление о регистрации TR_{kA} в базе данных. TR_{kA} определяют как соответствующую правилу или набору правил и электронно подписанную электронным устройством Алисы. Электронное устройство Кэрол затем электронно подписывает TR_{kA}. Полученная в результате запись транзакции далее называется как "$TR_{kA,kC1}$". $TR_{kA,kC1}$ затем регистрируют в базе данных.

Электронное устройство Боба затем получает уведомление о регистрации $TR_{kA,kC1}$ в базе данных. $TR_{kA,kC1}$ затем электронно подписывается электронным устройством Боба, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1,kB}$". $TR_{kA,kC1,kB}$ затем регистрируют в базе данных.

Электронное устройство Кэрол затем получает уведомление о регистрации $TR_{kA,kC1,kB}$ в базе данных. $TR_{kA,kC1,kB}$ определяют как электронно подписанное электронным устройством Боба. $TR_{kA,kC1,kB}$ затем электронно подписывается электронным устройством Кэрол, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1,kB,kC2}$". $TR_{kA,kC1,kB,kC2}$ затем регистрируют в базе данных. Электронное устройство Кэрол затем обеспечивает осуществление действия, где действие основано на информации о содержимом транзакции и связано с взиманием Кэрол налога.

Одним из преимуществ способа является то, что он уменьшает задержку (т.е. время ожидания) в процессе записи транзакции. Дополнительные преимущества способа станут очевидными из подробного описания ниже.

В одном варианте осуществления предусмотрена система регистрации в базе данных транзакции между первой стороной ("Алиса") и второй стороной ("Боб") и получения разрешения от третьей стороны ("Кэрол") на осуществление действия в отношении транзакции, при этом каждая из сторон Алиса, Боб и Кэрол имеет электронное устройство, выполненное с возможностью осуществления связи с базой данных посредством сети связи и выполненное с возможностью электронного подписывания данных, подлежащих отправке посредством сети связи. Система выполнена с возможностью осуществления этапов, как описано выше.

В других вариантах осуществления настоящее изобретение также относится к способам принятия участия в регистрации в базе данных такой транзакции и принятия участия в получении разрешения от третьей стороны ("Кэрол") на осуществление действия в отношении транзакции, при этом способы осуществляют с помощью одного из: электронного устройства Алисы, электронного устройства Кэрол и электронного устройства Боба.

В дальнейших вариантах осуществления настоящее изобретение, кроме того, относится к электронным устройствам для принятия участия в регистрации в базе данных такой транзакции и для принятия участия в получении разрешения от третьей стороны ("Кэрол") на осуществление действия в отношении транзакции, при этом в качестве электронных устройств используют любое из: электронного устройства Алисы, электронного устройства Кэрол и электронного устройства Боба.

Настоящее изобретение также относится к компьютерным программам или наборам компьютерных программ, включающим машиночитаемые команды, выполненные с возможностью, при осуществлении на электронном устройстве или наборе электронных устройств, приведения электронного устройства или набора электронных устройств к осуществлению любого из вышеописанных способов.

В некоторых вариантах осуществления, как определено, например, в зависимом пункте 6 формулы изобретения, транзакция относится к объекту, и объект маркируют кодом, представляющим собой или соответствующим идентификатору транзакции. Код, нанесенный на объект, затем могут считывать, например, когда объект отправлен Алисой, а затем могут определять путем запроса к базе данных, совпадает ли тип объекта с информацией о содержимом транзакции, идентифицируемой идентификатором транзакции, представленным или соответствующим считанному коду. Тип объекта может быть определен, например, визуальным осмотром объекта. Таким образом, в режиме реального времени или в режиме квазиреального времени транзакция может быть зарегистрирована, и позже может быть проверено, соответствует ли зарегистрированная транзакция фактической транзакции.

Краткое описание графических материалов

Варианты осуществления изобретения далее будут описаны в сочетании с прилагаемыми фигурами, на которых

фиг. 1a и 1b, которые следует рассматривать вместе, составляют схему последовательности способа в одном варианте осуществления настоящего изобретения;

на фиг. 2-5 представлены четыре блок-схемы способов в четырех вариантах осуществления настоящего изобретения;

фиг. 6a и 6b, которые следует рассматривать вместе, составляют схему последовательности способов в дополнительных вариантах осуществления настоящего изобретения;

на фиг. 7 представлена блок-схема способа согласно одному варианту осуществления настоящего изобретения; и

на фиг. 8 - схематический чертеж иллюстративного выполнения электронного устройства в одном варианте осуществления настоящего изобретения.

Подробное описание

Изобретение далее будет описано в сочетании с конкретными вариантами осуществления. Эти конкретные варианты осуществления служат для обеспечения лучшего понимания специалистом в данной области техники, но не предназначены для ограничения объема настоящего изобретения, который определен прилагаемой формулой изобретения. Перечень сокращений и их значения приведены в конце подробного описания в целях удобства.

Фиг. 1a и 1b, которые следует рассматривать вместе, составляют схему последовательности способа в одном варианте осуществления настоящего изобретения. Целью данного способа является, во-первых, регистрация, т.е. запись в базе данных транзакции между первой стороной и второй стороной и, во-вторых, получение разрешения от третьей стороны на осуществление действия в отношении транзакции. Первая, вторая и третья стороны (или, другими словами, субъекты) далее называются как Алиса, Боб и Кэрол, соответственно, исключительно в целях удобства.

База данных представляет собой компьютеризированную базу данных. Можно использовать множество видов компьютеризированных баз данных. В одном варианте осуществления база данных представляет собой распределенную базу данных. В одном варианте осуществления база данных представляет собой распределенный реестр (также называемый как технология "распределенного реестра"). В одном варианте осуществления база данных представляет собой распределенный разрешенный реестр. В одном варианте осуществления база данных представляет собой базу данных на основе блокчейна, такую как, например, общедоступная база данных на основе блокчейна или частная база данных на основе блокчейна (такая как, например, блокчейн, управляемый частным консорциумом). В одном варианте осуществления база данных представляет собой базу данных (или реестр), защищаемый блокчейном (как описано, например, в документе US 2017/0033932 A1). В одном варианте осуществления база данных является неизменной до определенной степени. Это означает, что после записи содержимого в базу данных очень трудно или очень хлопотно путем вычислений изменить указанное содержимое.

Каждая из сторон Алиса, Боб и Кэрол имеет электронное устройство, выполненное с возможностью осуществления связи с базой данных посредством сети связи. Могут использоваться многие виды электронных устройств, таких как, например, персональный компьютер, портативный компьютер, мобильный телефон, смартфон, планшетный компьютер, персональный цифровой помощник, переносной компьютер, игровое устройство, портативный медиаплеер, телевизионная приставка и/или камера. В одном варианте осуществления электронные устройства Алисы, Боба и Кэрол связаны между собой посредством одной или более сетей связи. Также могут использоваться многие виды сетей связи, например, без

ограничения Интернет и/или любые виды проводных или беспроводных сетей связи.

Каждое из электронных устройств Алисы, Боба и Кэрол выполнено с возможностью электронного подписывания данных от имени Алисы, Боба и Кэрол соответственно. Например, у каждой из сторон Алиса, Боб и Кэрол есть ключ, т.е. ключ, используемый для цифрового подписывания данных. В одном варианте осуществления каждый из ключей Алисы, Боба и Кэрол представляет собой личный ключ, и каждая из Алисы, Боба и Кэрол также имеет открытый ключ, оба ключа можно использовать вместе в рамках системы криптографии с открытым ключом или асимметричной криптографии.

В одном варианте осуществления электронное подписывание данных включает их цифровое подписывание с использованием ключа, такого как, например, личный ключ, как упомянуто выше.

В другом варианте осуществления электронное подписывание данных не включает использование ключа. Например, электронное подписывание данных может следовать из аутентификации пользователя, вводящего какие-либо учетные данные пользователя, такие как, например, имя пользователя и соответствующий пароль, или биометрические данные. После аутентификации данные могут затем добавляться в виде электронной подписи с данными подписи, указывающими, что аутентификация имела место.

В одном варианте осуществления транзакция включает продажу продукта или услуги. Например, Алиса может быть продавцом, Боб может быть покупателем, а Кэрол может быть налоговым органом.

Способ включает следующие этапы s2, s4, s6, s8, s10, s12, s14, s16, s18, s20, s22, s24, s26, s28 и s30, которые могут быть описаны поэтапно следующим образом со ссылкой на фиг. 1a и 1b. Далее, когда описано, что электронное устройство выполняет этап, этот этап может выполняться автоматически, например, с помощью одной или более компьютерных программ, выполняемых на электронном устройстве, или с помощью одной или более интегральных схем (или подобного) в электронном устройстве. В некоторых вариантах осуществления для одного или более этапов способа пользователю необязательно может потребоваться предоставить некоторый ввод для завершения этапа.

Этап s2.

На этапе s2 электронное устройство Алисы обеспечивает создание записи, далее называемой как "запись транзакции". Запись представляет собой структуру данных, которая может быть сохранена в базе данных.

В одном варианте осуществления запись транзакции создается электронным устройством Алисы.

В другом варианте осуществления (не проиллюстрировано на фиг. 1a) запись транзакции не создается сама по себе электронным устройством Алисы. В таком варианте осуществления электронное устройство Алисы может, например, передавать в базу данных параметры, необходимые для создания записи транзакции. База данных или компьютерная программа, связанная с или управляющая базой данных, затем создает запись транзакции. Например, компьютерная программа, управляющая базой данных, может включать набор команд, т.е. протокол, для создания записи транзакции. Запись транзакции или ее копия затем передается на электронное устройство Алисы для подписи (согласно этапу s4).

Запись транзакции представляет собой структуру данных, включающую: (i) идентификатор, далее называемый как "идентификатор транзакции", для идентификации транзакции, (ii) идентификатор для идентификации Алисы, (iii) идентификатор для идентификации Боба, и (iv) информацию, далее называемую как "информация о содержимом транзакции", относящуюся по меньшей мере к одному из: типа транзакции и ценности, которую, как полагают, имеет транзакция. Идентификаторы представляют собой уникальные идентификаторы, так что они эффективно обеспечивают на практике идентификацию транзакции Алисы и Боба соответственно.

В одном варианте осуществления запись транзакции может относиться к так называемому "смарт-контракту", так что создание записи транзакции может также относиться к инициации смарт-контракта. В одном варианте осуществления информация о содержимом транзакции включает описание продукта или услуги, его цену и налог на добавленную стоимость (НДС), также называемый как налог на товары и услуги (GST), применяемый к транзакции.

Этап s4.

На этапе s4 электронное устройство Алисы электронно подписывает запись транзакции, например, с помощью ключа Алисы. Полученная в результате запись транзакции, т.е. электронно подписанная запись транзакции, далее называется как "TR_{kA}". При электронном подписывании записи транзакции структура данных, составляющая запись транзакции, расширяется таким образом, что структура данных также включает электронную подпись. Другими словами, TR_{kA} включает, по меньшей мере, исходную запись транзакции (TR) (статус которой мог быть тем временем изменен) и электронную подпись записи транзакции, осуществляемую электронным устройством Алисы, например, с помощью ключа Алисы (kA).

Этап s6.

На этапе s6 (проиллюстрированном подэтапами s6.1 и s6.2 на фиг. 1a) TR_{kA} регистрируют, т.е. записывают, в базе данных. В одном варианте осуществления электронное устройство Алисы обеспечивает регистрацию TR_{kA} в базе данных.

В одном варианте осуществления регистрацию TR_{kA} в базе данных осуществляют посредством электронного устройства Алисы, как, например, посредством компьютерной программы, выполняемой на электронном устройстве Алисы в виде автоматической последовательности этапа s4 подписывания.

В другом варианте осуществления регистрацию TR_{kA} в базе данных не осуществляют посредством электронного устройства Алисы самого по себе, но перенаправляют на другое электронное устройство в виде автоматической последовательности операции s4 подписывания. Например, регистрацию TR_{kA} в базе данных могут перенаправлять на компьютерную программу, связанную с базой данных.

Этап s8.

На этапе s8 электронное устройство Кэрол затем получает уведомление о регистрации TR_{kA} в базе данных.

В одном варианте осуществления (не проиллюстрировано на фиг. 1a) TR_{kA} передают на электронное устройство Кэрол. TR_{kA} могут передавать на электронное устройство Кэрол, например, посредством электронного устройства Алисы, или посредством базы данных, или посредством компьютерной программы, связанной с или управляющей базой данных. Например, компьютерная программа, управляющая базой данных, может включать набор команд, т.е. протокол, для передачи TR_{kA}. Однако настоящее изобретение не ограничено данными вариантами реализации. Например, в еще одном варианте реализации может быть необходимо электронное устройство Боба для подтверждения транзакции перед отправкой TR_{kA} на электронное устройство Кэрол.

Передачу TR_{kA} на электронное устройство Кэрол могут осуществлять с помощью любого типа сообщения.

В другом варианте осуществления TR_{kA} саму по себе не передают на электронное устройство Кэрол, а только информацию о том, что TR_{kA} доступна, т.е. была зарегистрирована, в базе данных, передают на электронное устройство Кэрол. Таким образом, электронное устройство Кэрол информируют о том, что запись транзакции была создана, была электронно подписана электронным устройством Алисы и готова к электронному подписыванию электронным устройством Кэрол. Информация о регистрации TR_{kA} в базе данных может быть передана на электронное устройство Кэрол, например, электронным устройством Алисы (не проиллюстрировано на фиг. 1a), или базой данных (как проиллюстрировано на фиг. 1a), или компьютерной программой, связанной с или управляющей базой данных.

Например, компьютерная программа, управляющая базой данных, может включать набор команд, т.е. протокол, для передачи указанной информации. Однако настоящее изобретение не ограничено данными вариантами реализации. Например, в еще одном варианте реализации может быть необходимо электронное устройство Боба для подтверждения транзакции перед отправкой уведомления на электронное устройство Кэрол (не проиллюстрировано на фиг. 1a).

Отправку уведомления на электронное устройство Кэрол о регистрации TR_{kA} в базе данных могут осуществлять посредством любого типа сообщения.

Этап s10.

На этапе s10 TR_{kA} определяют как соответствующую правилу или набору правил и электронно подписанную электронным устройством Алисы.

Этап s10 могут осуществлять электронным устройством Кэрол (например, после извлечения TR_{kA} из базы данных, если она еще не доступна для электронного устройства Кэрол), или базой данных, или компьютерной программой, связанной с или управляющей базой данных. В качестве альтернативы, осуществление этапа s10 могут даже делегировать на еще один элемент сети.

В одном варианте осуществления этап s10 осуществляют, как только электронное устройство Кэрол получает уведомление о регистрации TR_{kA} в базе данных.

В одном варианте осуществления, если определяют, что TR_{kA} не соответствует правилу или набору правил и/или не была электронно подписана электронным устройством Алисы, весь процесс, например, может быть прерван.

Этап s12.

Затем на этапе s12 TR_{kA} дополнительно электронно подписывают электронным устройством Кэрол, например, с помощью ключа Кэрол. Таким образом, электронное устройство Кэрол электронно подписывает TR_{kA}. Полученная в результате запись транзакции, т.е. дополнительно электронно подписанная запись транзакции, далее называется как "$TR_{kA,kC1}$".

$TR_{kA,kC1}$ включает, по меньшей мере, исходную запись транзакции TR_{kA} (статус которой мог измениться за это время) и электронную подпись TR_{kA} электронным устройством Кэрол, например, с помощью ключа Кэрол (kC).

Этап s14.

На этапе s14 (проиллюстрированном подэтапами s14.1 и s14.2 на фиг. 1a) $TR_{kA,kC1}$ регистрируют, т.е. записывают, в базе данных. В одном варианте осуществления электронное устройство Кэрол обеспечивает регистрацию $TR_{kA,kC1}$ в базе данных.

В одном варианте осуществления регистрацию $TR_{kA,kC1}$ в базе данных осуществляют посредством электронного устройства Кэрол, как, например, посредством компьютерной программы, выполняемой на электронном устройстве Кэрол в виде автоматической последовательности операции s12 подписывания.

В другом варианте осуществления регистрацию $TR_{kA,kC1}$ в базе данных не осуществляют посредством электронного устройства Кэрол самого по себе, а посредством другого электронного устройства в виде автоматической последовательности этапа s12 подписывания.

Этап s16.

На этапе s16 электронное устройство Боба затем получает уведомление о регистрации $TR_{kA,kC1}$ в базе данных.

В одном варианте осуществления (не проиллюстрировано на фиг. 1a) $TR_{kA,kC1}$ передают на электронное устройство Боба. $TR_{kA,kC1}$ могут передавать на электронное устройство Боба, например, посредством электронного устройства Кэрол, или посредством базы данных, или посредством компьютерной программы, связанной с или управляющей базой данных. Однако настоящее изобретение не ограничено данными вариантами реализации.

Передачу $TR_{kA,kC1}$ на электронное устройство Боба могут осуществлять с помощью любого типа сообщения.

В другом варианте осуществления $TR_{kA,kC1}$ саму по себе не передают на электронное устройство Боба, а только информацию о том, что $TR_{kA,kC1}$ доступна, т.е. была зарегистрирована, в базе данных, передают на электронное устройство Боба. Таким образом, электронное устройство Боба информируют о том, что запись транзакции была создана и готова к электронному подписыванию электронным устройством Боба. Информация о регистрации $TR_{kA,kC1}$ в базе данных может быть передана на электронное устройство Боба, например, электронным устройством Кэрол (не проиллюстрировано на фиг. 1a), или базой данных (как проиллюстрировано на фиг. 1a), или компьютерной программой, связанной с или управляющей базой данных. Однако настоящее изобретение не ограничено данными вариантами реализации.

Отправку уведомления на электронное устройство Боба о регистрации $TR_{kA,kC1}$ в базе данных могут осуществлять посредством любого типа сообщения.

Этап s18.

На этапе s18 $TR_{kA,kC1}$ дополнительно электронно подписывают электронным устройством Боба, например, с помощью ключа Боба. Таким образом, электронное устройство Боба электронно подписывает $TR_{kA,kC1}$. Это могут, например, осуществлять после извлечения $TR_{kA,kC1}$ из базы данных, если она еще не доступна для электронного устройства Боба. Полученная в результате запись транзакции, т.е. дополнительно электронно подписанная запись транзакции, далее называется как "$TR_{kA,kC1,kB}$".

$TR_{kA,kC1,kB}$ включает, по меньшей мере, исходную запись транзакции $TR_{kA,kC1}$ (статус которой мог измениться за это время) и электронную подпись $TR_{kA,kC1}$ электронным устройством Боба.

В одном варианте осуществления электронное устройство Боба электронно подписывает $TR_{kA,kC1}$, только если Боб соглашается на транзакцию, либо путем получения согласия Боба (посредством взаимодействия с пользовательским интерфейсом), либо путем применения набора правил на электронном устройстве Боба (например, в форме программно-реализованного определения). Если Боб не согласен на транзакцию, весь процесс может быть прерван или прекращен.

В одном варианте осуществления подтверждение транзакции может быть отложено до тех пор, пока Боб не убедится, что транзакция состоялась или будет иметь место, например, до тех пор, пока Боб не убедится, что объект или услуга были или будут должным образом доставлены или предоставлены.

Этап s20.

На этапе s20 (проиллюстрированном подэтапами s20.1 и s20.2 на фиг. 1b) $TR_{kA,kC1,kBA}$ регистрируют, т.е. записывают, в базе данных. В одном варианте осуществления электронное устройство Боба обеспечивает регистрацию $TR_{kA,kC1,kB}$ в базе данных.

В одном варианте осуществления регистрацию $TR_{kA,kC1,kB}$ в базе данных осуществляют посредством электронного устройства Боба, как, например, посредством компьютерной программы, выполняемой на электронном устройстве Боба в виде автоматической последовательности этапа s18 подписывания.

В другом варианте осуществления регистрацию $TR_{kA,kC1,kB}$ в базе данных не осуществляют посредством электронного устройства Боба самого по себе, а посредством другого электронного устройства в виде автоматической последовательности этапа s18 подписывания.

Этап s22.

На этапе s22 электронное устройство Кэрол затем получает уведомление о регистрации $TR_{kA,kC1,kB}$ в базе данных.

В одном варианте осуществления (не проиллюстрировано на фиг. 1b) $TR_{kA,kC1,kB}$ передают на электронное устройство Кэрол. $TR_{kA,kC1,kB}$ могут передавать на электронное устройство Кэрол, например, посредством электронного устройства Боба, или посредством базы данных, или посредством компьютерной программы, связанной с или управляющей базой данных. Однако, настоящее изобретение не ограничено данными вариантами реализации.

Передачу $TR_{kA,kC1,kB}$ на электронное устройство Кэрол могут осуществлять с помощью любого типа сообщения.

В другом варианте осуществления $TR_{kA,kC1,kB}$ саму по себе не передают на электронное устройство Кэрол, а только информацию о том, что $TR_{kA,kC1,kB}$ доступна, т.е. была зарегистрирована, в базе данных, передают на электронное устройство Кэрол. Таким образом, электронное устройство Кэрол получает информацию о готовности $TR_{kA,kC1,kB}$ к электронному подписыванию электронным устройством Кэрол. Информация о регистрации $TR_{kA,kC1,kB}$ в базе данных может быть передана на электронное устройство Кэрол, например, электронным устройством Боба (не проиллюстрировано на фиг. 1b), или базой данных

(как проиллюстрировано на фиг. 1b), или компьютерной программой, связанной с или управляющей базой данных. Однако настоящее изобретение не ограничено данными вариантами реализации.

Отправку уведомления на электронное устройство Кэрол о регистрации $TR_{kA,kC1,kB}$ в базе данных могут осуществлять посредством любого типа сообщения.

Этап s24.

На этапе s24 $TR_{kA,kC1,kB}$ определяют как электронно подписанную электронным устройством Боба.

Данное определение могут осуществлять электронным устройством Кэрол (например, после извлечения $TR_{kA,kC1,kB}$ из базы данных, если она еще не доступна для электронного устройства Кэрол), или базой данных, или компьютерной программой, связанной с или управляющей базой данных. Осуществление этапа s24 могут даже делегировать на еще один элемент сети.

В одном варианте осуществления этап s24 осуществляют, как только электронное устройство Кэрол получает уведомление о регистрации $TR_{kA,kC1,kB}$ в базе данных.

В одном варианте осуществления, если определяют, что $TR_{kA,kC1,kB}$ не была электронно подписана электронным устройством Боба, весь процесс, например, может быть прерван или прекращен.

Этап s26.

Затем на этапе s26 $TR_{kA,kC1,kB}$ дополнительно электронно подписывают электронным устройством Кэрол, например, с помощью ключа Кэрол. Таким образом, электронное устройство Кэрол электронно подписывает $TR_{kA,kC1,kB}$. Полученная в результате запись транзакции, т.е. дополнительно электронно подписанная запись транзакции, далее называется как "$TR_{kA,kC1,kB,kC2}$".

$TR_{kA,kC1,kB,kC2}$ включает по меньшей мере исходную запись транзакции $TR_{kA,kC1,kB}$ (статус которой мог измениться за это время) и электронную подпись $TR_{kA,kC1,kB}$ электронным устройством Кэрол. Другими словами, электронная подпись $TR_{kA,kC1,kB}$ электронным устройством Кэрол, как правило, отличается от электронной подписи TR_{kA} электронным устройством Кэрол (см. этап s12 выше), поскольку данные, которые электронно подписаны, отличаются.

Этап s28.

На этапе s28 (проиллюстрирован подэтапами s28.1 и s28.2 на фиг. 1b) $TR_{kA,kC1,kB,kC2}$ затем регистрируют в базе данных. В одном варианте осуществления электронное устройство Кэрол обеспечивает регистрацию $TR_{kA,kC1,kB,kC2}$ в базе данных.

В одном варианте осуществления регистрацию $TR_{kA,kC1,kB,kC2}$ в базе данных осуществляют посредством электронного устройства Кэрол, как, например, посредством компьютерной программы, выполняемой на электронном устройстве Кэрол в виде автоматической последовательности этапа s26 подписывания.

В другом варианте осуществления регистрацию $TR_{kA,kC1,kB,kC2}$ в базе данных не осуществляют посредством электронного устройства Кэрол самого по себе, а посредством другого электронного устройства в виде автоматической последовательности этапа s26 подписывания.

Этап s30.

На этапе s30 осуществление действия обеспечивают электронным устройством Кэрол. Действие основано на информации о содержимом транзакции, т.е. вызванное действие зависит от информации о содержимом транзакции. Кроме того, действие связано с взиманием Кэрол налога.

Таким образом, способ уменьшает задержку (т.е. время ожидания) в процессе записи транзакции в базе данных (этапы s2-s28), что приводит к выполнению действия на основе информации о содержимом транзакции (этап s30). Таким образом, способ обеспечивает техническое решение для отслеживания транзакций в режиме реального времени (т.е. с малой задержкой) и для каждой отдельной транзакции. Отслеживание может быть осуществлено третьей стороной, т.е. Кэрол.

В одном варианте осуществления электронное подписывание записи транзакции также включает присвоение метки времени к записи транзакции, т.е. добавление метки времени к структуре данных записи транзакции.

В одном варианте осуществления определение s10 того, что TR_{kA} соответствует правилу или набору правил, включает верификацию электронным устройством Кэрол на основе идентификатора для идентификации Алиса, идентификатора для идентификации Боб и информации о содержимом транзакции соответствия транзакции правилу или набору правил. Это может, например, включать верификацию того, что вся необходимая информация была включена в запись транзакции, что транзакция авторизована и что выбранная ставка НДС является правильной.

В одном варианте осуществления запись транзакции дополнительно включает параметр состояния, указывающий по меньшей мере на одно из того: (a) что запись транзакции была электронно подписана (этап s4) электронным устройством Алисы; (b) что TR_{kA} была зарегистрирована (этап s6) в базе данных; (c) что электронное устройство Кэрол получило уведомление (этап s8) о регистрации TR_{kA} в базе данных; (d) что TR_{kA} была определена (этап s10) как соответствующая правилу или набору правил и электронно подписанная электронным устройством Алисы; (e) что TR_{kA} была электронно подписана (этап s12) электронным устройством Кэрол; (f) что $TR_{kA,kC1}$ была зарегистрирована (этап s14) в базе данных; (g) что электронное устройство Боба получило уведомление (этап s16) о регистрации $TR_{kA,kC1}$ в базе данных; (h) что $TR_{kA,kC1}$ была электронно подписана (этап s18) электронным устройством Боба; (i) что $TR_{kA,kC1,kB}$ была зарегистрирована (этап s20) в базе данных; (j) что электронное устройство Кэрол получило уведомле-

ние (этап s22) о регистрации $TR_{kA,kC1,kB}$ в базе данных; (k) что $TR_{kA,kC1,kB}$ была определена (этап s24) как электронно подписанная электронным устройством Боба; (l) что $TR_{kA,kC1,kB}$ была электронно подписана (этап s26) электронным устройством Кэрол; (m) что $TR_{kA,kC1,kB,kC2}$ была зарегистрирована (этап s28) в базе данных; и (n) что было обеспечено осуществление (этап s30) действия. В одном варианте осуществления параметр состояния указывает на истинность или ложность каждого из (a)-(n).

Таким образом, параметр состояния позволяет любой авторизованной стороне при получении или просмотре записи транзакции выяснить, какая из вышеуказанных операций (a)-(n) была осуществлена. Другими словами, статус записи транзакции регистрируют в базе данных в виде части записи транзакции.

В одном варианте осуществления транзакция относится к объекту, и объект маркируют кодом, представляющим собой или соответствующим идентификатору транзакции. Объект могут, например, маркировать кодом немедленно или сразу же после создания записи транзакции. Код могут наносить на любую часть объекта, как, например, на упаковку, окружающую сердцевину объекта.

Объект может быть объектом любого типа, таким как, например, без ограничения бутылка или банка пива, вина, спиртного напитка или безалкогольного напитка, пачка, упаковка или коробка сигарет или сигар, медицинская упаковка, флакон духов или любые другие подакцизные товары, карта, билет, этикетка, бандероль, защитная фольга, защитная нить или т.п.

Код представляет собой машиночитаемый код, который может, например, включать по меньшей мере один из линейного штрих-кода и матричного штрих-кода (например, напечатанного двумерного матричного штрих-кода или QR-кода). Код может представлять собой идентификатор транзакции или может соответствовать идентификатору транзакции. Соответствие между кодом и идентификатором транзакции может представлять собой математическое соотношение (математически выводимое соответствие) или может храниться в базе данных (зарегистрированное соответствие).

В одном варианте осуществления, в котором транзакция относится к объекту и в котором объект маркируют кодом, представляющим собой или соответствующим идентификатору транзакции, способ дополнительно включает следующие этапы, как проиллюстрировано блок-схемой согласно фиг. 2. Код, нанесенный на объект, считывают s32a, например, устройством для считывания штрих-кода или тому подобным. Затем определяют (s34a) путем запроса к базе данных по меньшей мере одно из того: (i) осуществлено ли действие (относящееся к этапу s30) для транзакции, идентифицируемой идентификатором транзакции, представляющим собой или соответствующим считанному коду; и (ii) совпадает ли тип объекта с информацией о содержимом транзакции, идентифицируемой идентификатором транзакции, представленным или соответствующим считанному коду.

В одном варианте осуществления транзакция относится к услуге, и документ, связанный с услугой, маркируют кодом, представляющим собой или соответствующим идентификатору транзакции. Документ может, например, быть маркирован кодом после создания записи транзакции, как, например, немедленно или сразу же после создания записи транзакции.

Как упомянуто выше, код представляет собой машиночитаемый код, который может, например, включать по меньшей мере один из линейного штрих-кода и матричного штрих-кода (например, напечатанного двумерного матричного штрих-кода или QR-кода).

В одном варианте осуществления, в котором транзакция относится к услуге, и в котором документ, связанный с услугой, маркируют кодом, представляющим собой или соответствующим идентификатору транзакции, способ дополнительно включает следующие этапы, как проиллюстрировано блок-схемой согласно фиг. 3, например, устройством для считывания штрих-кода или тому подобным. Считывают s32b код, нанесенный на документ, связанный с услугой. Затем определяют (s34b) путем запроса к базе данных по меньшей мере одно из того: (iii) осуществлено ли действие (относящееся к этапу s30) для транзакции, идентифицируемой идентификатором транзакции, представленным или соответствующим считанному коду; и (iv) совпадает ли тип объекта с информацией о содержимом транзакции, идентифицируемой идентификатором транзакции, представленным или соответствующим считанному коду.

В одном варианте осуществления транзакция относится к объекту, и идентификатор транзакции соответствует подписи, далее называемой как "подпись объекта", генерируемой на основе по меньшей мере одного из: свойства объекта и свойства защитного элемента на основе материала, наносимого на или прикрепляемого к объекту.

Приведенные выше замечания относительно иллюстративного типа объекта также применимы к настоящему варианту осуществления.

В этом варианте осуществления способ может дополнительно включать следующие этапы, как проиллюстрировано блок-схемой согласно фиг. 4. Получают s32c подпись объекта с использованием подходящего устройства для считывания. Затем определяют (s34c) путем запроса к базе данных по меньшей мере одно из того: (v) осуществлено ли действие (относящееся к этапу s30) для транзакции, идентифицируемой идентификатором транзакции, соответствующим полученной подписи объекта; и (vi) совпадает ли тип объекта с информацией о содержимом транзакции, идентифицируемой идентификатором транзакции, соответствующим полученной подписи объекта.

В одном варианте осуществления транзакция относится к услуге, и идентификатор транзакции соответствует подписи, далее называемой как "подпись документа, связанного с услугой", генерируемой на

основе по меньшей мере одного из: свойства документа, связанного с услугой, и свойства защитного элемента на основе материала, наносимого на или прикрепляемого к документу, связанному с услугой.

В этом варианте осуществления способ может дополнительно включать следующие этапы, как проиллюстрировано блок-схемой согласно фиг. 5. Получают s32d подпись документа, связанного с услугой, с использованием подходящего устройства для считывания. Затем определяют (s34d) путем запроса к базе данных по меньшей мере одно из того: (vii) осуществлено ли действие (относящееся к этапу s30) для транзакции, идентифицируемой идентификатором транзакции, соответствующим полученной подписи документа, связанного с услугой; и (viii) совпадает ли тип объекта с информацией о содержимом транзакции, идентифицируемой идентификатором транзакции, соответствующим полученной подписи документа, связанного с услугой.

Фиг. 6a и 6b, которые следует рассматривать вместе, составляют схему последовательности способов в четырех вариантах осуществления настоящего изобретения. Способы отличаются от способа, проиллюстрированного на фиг. 1a и 1b в том, что они включают следующие дополнительные этапы.

В первом варианте осуществления (как рассмотрено, например, со ссылкой на фиг. 2) объект, к которому относится транзакция, маркируют s7 кодом (см. фиг. 6a, этап s7, "(i) маркировка кода"). После этого этапа физической маркировки объекта кодом, код объекта могут позже считывать s32, а определение отслеживания и контроля могут осуществлять s34 путем запроса к базе данных (см. фиг. 6b, этапы s32-s34, "считывание и проверка").

Во втором варианте осуществления (как рассмотрено, например, со ссылкой на фиг. 3) документ, связанный с услугой, к которой относится транзакция, маркируют s7 кодом (см. фиг. 6a, этап s7, "(i) маркировка кода"). После этого этапа физической маркировки документа кодом, код документа могут считывать s32, а определение отслеживания и контроля могут затем осуществлять s34 путем запроса к базе данных (см. фиг. 6b, этапы s32-s34, "считывание и проверка").

В третьем варианте осуществления (как рассмотрено, например, со ссылкой на фиг. 4) генерируют s7 подпись объекта, к которому относится транзакция (см. фиг. 6a, этап s7, "(ii) генерирование "подписи объекта""). После генерирования подписи объекта, т.е. физической подписи объекта, может быть получена s32 подпись объекта, и затем определение отслеживания и контроля могут осуществлять s34 путем запроса к базе данных (см. фиг. 6b, этапы s32-s34, "считывание и проверка").

В четвертом варианте осуществления (как рассмотрено, например, со ссылкой на фиг. 5) генерируют s7 подпись документа, связанного с услугой, к которой относится транзакция (см. фиг. 6a, этап s7, "(iii) генерирование подписи документа, связанного с услугой"). После генерирования указанной подписи документа, связанного с услугой, т.е. физической подписи документа, затем могут получить s32 подпись документа, связанного с услугой, а определение отслеживания и контроля затем могут осуществлять s34 путем запроса к базе данных (см. фиг. 6b, этапы s32-s34, "считывание и проверка").

Алиса или операторы Алисы осуществляют или, по меньшей мере, управляют этапом s7, как проиллюстрировано пунктирной стрелкой от Алисы до поля, иллюстрирующего этап s7. Этап s7 могут осуществлять в любое время после этапа s2. Кэрол или операторы Кэрол осуществляют или, по меньшей мере, управляют этапами s32-s34 в полевых условиях, как проиллюстрировано пунктирной стрелкой от Кэрол до поля, иллюстрирующего этапы s32-s34.

В одном варианте осуществления любая из вышеупомянутой подписи объекта и вышеупомянутой подписи документа, связанного с услугой, содержит защитный элемент на основе материала. Защитный элемент на основе материала представляет собой элемент, включающий материал, особенность которого, относящаяся к его конкретному типу и соотношению, позволяет материально установить подлинность маркированного элемента, просто обнаруживая указанную особенность. Особенность этого материала составляет подпись материала маркировки. Например, защитный элемент на основе материала может быть выполнен в виде люминесцентного материала. Люминесценцию могут обнаружить при невидимом свете, например ультрафиолетовом свете или инфракрасном свете. В качестве альтернативы, могут обнаружить люминесценцию при применении видимого света. Люминесцентный материал может представлять собой люминесцентный материал преобразования с повышением частоты или люминесцентный материал преобразования с понижением частоты. Люминесцентный материал может представлять собой фосфоресцентный или флуоресцентный материал, в частности, в сочетании с периодом полураспада или другой характеристикой материала времени распада. Маркировка может быть напечатана краской, включающей указанный люминесцентный материал (в виде люминесцентных пигментов). Определенное устройство для считывания может быть необходимо для обнаружения подписи материала на маркировке, включающей заданный защитный элемент на основе материала: например, в случае флуоресцентной краски, устройство для считывания должно осветить краску приемлемым возбуждающим светом, а затем обнаружить люминесцентный свет, испускаемый краской, и, например, быть выполненным с возможностью обнаружения и измерения скорости распада (т.е. физической характеристики) этого люминесцентного света.

Варианты осуществления, проиллюстрированные со ссылкой на фиг. 2-6, позволяют реализовать эффективное решение по отслеживанию и контролю в сочетании со способом регистрации транзакции в базе данных. Другими словами, физическая маркировка на объектах и/или документах, связанных с ус-

лугами, или их подпись материала, в частности, позволяет выяснить состояние транзакции путем запроса к базе данных. В частности, может быть идентифицировано, было ли действие должным образом выполнено, и/или может быть идентифицировано, совпадает ли тип объекта с ожидаемым типом объекта в соответствии с информацией в базе данных. Это может позволить обнаружить мошенничество.

Действие вышеописанного этапа s30 связано с взиманием Кэрол налога, такого как, например, НДС или GST.

Как упомянуто выше, способ, проиллюстрированный со ссылкой на фиг. 1a и 1b, уменьшает задержку в процессе записи транзакции в базе данных, что приводит к выполнению действия на основе информации о содержимом транзакции. Таким образом, способ обеспечивает техническое решение для отслеживания транзакций в режиме реального времени (т.е. с малой задержкой) и для каждой отдельной транзакции. Это имеет значительные сопутствующие преимущества, когда действие этапа s30 связано с взиманием налога, такого как, например, НДС или GST. Это можно объяснить следующим образом.

На момент написания сбор НДС в большинстве стран в основном возложен на всех экономических субъектов, при условии, что каждый субъект будет должным образом соблюдать применимые правила. Для обеспечения соблюдения правил налоговый орган проводит проверки, а штрафы и пени используются для предотвращения мошенничества, но с ограниченным успехом. Действительно, в процессе сбора НДС участвуют многие субъекты с миллионами (если не миллиардами) транзакций, так что налоговому органу практически невозможно предотвратить мошенничество. Примером мошенничества с НДС является несоответствие одного и того же счета со стороны продавца и со стороны покупателя. В частности, псевдопокупатель может выставить фальшивый счет за товар, который никогда не был куплен, требуя возмещение НДС за несуществующую покупку. Кроме того, на обычный сбор НДС влияет внутренняя задержка, обусловленная как составлением счетов на основе бухгалтерского учета, так и юридическими требованиями, согласно которым экономические субъекты должны выдавать декларации НДС только периодически (например, каждый месяц, каждый квартал или каждый год).

Когда действие этапа s30 связано с взиманием налога, решение, описанное со ссылкой на фиг. 1a и 1b, предоставляет технические средства для записи, отслеживания, отчетности, расчета и аудита транзакций, являющихся объектами налогообложения НДС, между доверенными сторонами, т.е. Алисой, которая может быть продавцом, Бобом, который может быть покупателем, и Кэрол, которая может быть налоговым органом. Это может быть достигнуто путем замены обычных счетов НДС записями транзакций в базе данных, чтобы автоматически записывать, отслеживать и рассчитывать соответствующие транзакции, являющиеся объектами налогообложения НДС, для каждой отдельной транзакции и с малой задержкой. Например, транзакция, являющаяся объектом налогообложения НДС, может быть зашифрована в так называемый смарт-контракт, автоматически выполняющий расчет НДС между различными сторонами в базе данных на основе блокчейна.

В одном варианте осуществления при электронном подписывании TR_{kA} электронным устройством Кэрол (этап s12), например, с помощью ключа Кэрол, счет, связанный с Алисой, списывают с суммы, представляющей собой налог на добавленную стоимость, которая считается результатом транзакции; и при определении (s24) того, что $TR_{kA,kC1,kB}$ была электронно подписана электронным устройством Боба, счет, связанный с Бобом, пополняют на эту сумму. Другими словами, в этом варианте осуществления подпись Кэрол приводит к списыванию со счета Алисы, и определение того, что $TR_{kA,kC1,kB}$ была электронно подписана электронным устройством Боба, приводит к пополнению счета Боба.

Преимущество такого варианта осуществления заключается в том, что налог, такой как НДС, может взиматься (или учитываться) для каждой отдельной транзакции, автоматически и с малой задержкой, таким образом, чтобы снизить возможности для совершения мошенничества (как, например, так называемое мошенничество с отсутствующим трейдером и "карусельное мошенничество"). Компания (обычно небольшая) не сможет внезапно генерировать совершенно ненормальное количество транзакций (относительно ее размера и типа бизнеса) в течение недель или месяцев, таким образом, из-за очень большой суммы НДС, налоговому органу (и затем внезапно исчезать без уплаты причитающихся сумм) до следующей подачи налоговой декларации. С помощью вышеописанных способа и системы для каждой отдельной транзакции налоговый орган может в режиме реального времени увидеть уровень НДС, причитающийся каждой компании, и может обнаружить потенциального мошенника и вмешаться до того, как компания накопит ненормальные долги по НДС.

В другом варианте осуществления счет, связанный с Алисой, списывают с суммы, представляющей собой налог на добавленную стоимость, которая считается результатом транзакции только после электронного подписывания $TR_{kA,kC1,kB}$ электронным устройством Боба, а не до этого.

На фиг. 7 представлена блок-схема способа в дополнительном варианте осуществления настоящего изобретения. Способ включает следующие этапы.

На основе так называемого шаблона T200 смарт-контракта (т.е. шаблона для создания записи транзакции) (см. подэтап s2.1 на фиг. 7) и на основе идентификатора T390 смарт-контракта (т.е. идентификатора транзакции) (см. подэтап s2.2 на фиг. 7) создают T210 смарт-контракт (т.е. запись транзакции). Алиса может затем вводить T220 параметры в смарт-контракт (см. подэтап s2.3 на фиг. 7). (Это соответствует этапу s2, рассматриваемому, например, со ссылкой на фиг. 1a).

Затем электронное устройство Алисы электронно подписывает T230 смарт-контракт (который становится TR_{kA}), прежде чем передать его T240 в базу данных T380, которая, например, может быть неизменным реестром. (Это соответствует этапам s4 и s6, рассматриваемым, например, со ссылкой на фиг. 1a).

Уведомление T250 о регистрации смарт-контракта в базе данных затем отправляют на электронное устройство Кэрол. (Это соответствует этапу s8, рассматриваемому, например, со ссылкой на фиг. 1a.)

Затем электронное устройство Кэрол осуществляет T260 проверку соответствия и верифицирует T260, был ли смарт-контракт должным образом подписан электронным устройством Алисы. (Это соответствует этапу s10, рассматриваемому, например, со ссылкой на фиг. 1a). При неудачном определении T260 процесс может, например, вернуться к этапу T220. При успешном определении T260 электронное устройство Кэрол затем электронно подписывает T270 смарт-контракт (который становится $TR_{kA,kC1}$) и передает его в базу данных T380. (Это соответствует этапам s12 и s14, рассматриваемым, например, со ссылкой на фиг. 1a.) Электронное устройство Кэрол (налоговый орган) затем списывает T280 налоговый счет Алисы.

Уведомление T290 о регистрации смарт-контракта в базе данных затем отправляют на электронное устройство Боба. (Это соответствует этапу s16, рассматриваемому, например, со ссылкой на фиг. 1a.)

Электронное устройство Боба затем электронно подписывает T300 смарт-контракт (который становится $TR_{kA,kC1,kB}$) и передает его в базу данных T380. (Это соответствует этапам s18 и s20, рассматриваемым, например, со ссылкой на фиг. 1a и 1b.)

Уведомление T310 о регистрации смарт-контракта в базе данных затем отправляют на электронное устройство Кэрол, т.е. налоговый орган. (Это соответствует этапу s22, рассматриваемому, например, со ссылкой на фиг. 1b.) Затем электронное устройство Кэрол верифицирует T320, был ли смарт-контракт подписан электронным устройством Боба. (Это соответствует этапу s24, рассматриваемому, например, со ссылкой на фиг. 1b.) При неудачном определении T320 процесс может, например, вернуться к этапу T220. При успешном определении T320 электронное устройство Кэрол затем электронно подписывает T3ЗО смарт-контракт (который становится $TR_{kA,kC1,kB,KC2}$) и передает его в базу данных T380. (Это соответствует этапам s26 и s28, рассматриваемым, например, со ссылкой на фиг. 1b.) Электронное устройство Кэрол (налоговый орган) затем пополняет T280 налоговый счет Боба. Затем транзакция считается завершенной T350/s31.

Вышеописанные этапы могут рассматриваться как формирующие "цифровую часть" T360 способа и системы. Параллельно часть T370 "физической маркировки" также показана на правой стороне фиг. 7. В этой части код T400/s7.1 (идентификатор смарт-контракта) может быть нанесен на объект s7.2, на счет T410/s7.3 и даже на упаковку, содержащую соответствующие объекты s7.4. (Это соответствует этапу s7, рассматриваемому, например, со ссылкой на фиг. 6a). Позже может быть осуществлена s32/s34 проверка отслеживания и контроля от имени налогового органа, как рассмотрено, например, со ссылкой на фиг. 6b.

Благодаря вышеописанному способу налоговый орган (т.е. Кэрол) может в режиме реального времени (т.е. с малой задержкой) отслеживать статус налогового кредита любого налогоплательщика (т.е. Алисы и Боба). Для этого можно обратиться к базе данных (например, реестру блокчейна), что позволяет объединить все дебетовые и кредитные операции, назначенные Алисе, как результат всех предыдущих транзакций, а также эффективные платежи от Алисы и к Алисе. Для любого налогоплательщика, которого подозревают в мошенничестве, такого как, например, Алиса, налоговый орган может установить максимальные пределы задолженности по налогам (например, пороговое значение). Если Алиса достигает этого предела и хочет создать новые транзакции (т.е. чтобы выставить счет на новые продажи), налоговый орган может предпринять некоторые действия, прежде чем разрешить дальнейшие транзакции. Эти действия могут, например, включать отправку аудитора в служебные помещения Алисы, запрос гарантий от Алисы (например, гарантии от банка) для предотвращения более высокой задолженности по налогам, уменьшая текущий долг путем платежа и т. д. Может даже рассматриваться блокирование любой дальнейшей транзакции.

Кроме того, для каждой транзакции налоговый орган (Кэрол) может проверять существование продавца (Алиса) и покупателя (Боб) в официальном реестре налогоплательщиков. Разрешения на подпись лиц, которые электронно подписывают от имени своих юридических компаний (Алиса или Боб), также могут быть проверены в официальном реестре налогоплательщиков и/или коммерческом реестре.

Более того, может быть проверена актуальность данных, введенных Алисой в смарт-контракт. Это может, например, включать следующее: (i) соответствует ли класс налога (т.е. применяемая налоговая ставка) описанным товарам (например, пониженная налоговая ставка, применяемая к продуктам питания, не обязательно действительна для предметов роскоши); (ii) зарегистрированы ли Алиса и Боб в качестве налогоплательщиков; и (iii) указана ли стоимость транзакции.

Кроме того, можно проверить, правда ли электронные подписи действительны (т.е. они соответствуют авторизованным подписантам компаний Алисы или Боба).

Более того, анализ данных, содержащихся в базе данных, позволяет обнаружить потенциальные мошеннические действия со стороны налогоплательщиков (например, Алисы или Боба). Это может быть сделано путем распознавания определенных шаблонов или определенной комбинации шаблонов, таких как:

а) небольшие компании;

b) недавно приобретенные компании;

c) недавние изменения в правлении и/или руководстве компании;

d) частая смена лица, подписывающего транзакции (относительно размера компании);

e) бизнес за пределами обычной сферы деятельности компании (например, ресторан, начинающий продавать электронные товары);

f) объем продаж внезапно становится очень важным;

g) покупки в другой стране (импорт);

h) несвоевременные выплаты причитающихся налогов.

При подозрении в мошенничестве налоговый орган может инициировать различные виды действий:

i) простой запрос объяснений;

j) физический осмотр помещений компании;

k) физический аудит персонала компании, директоров и правления;

l) физический осмотр товаров в помещениях Алисы и/или Боба;

m) физический осмотр товаров при отгрузке (по всей цепочке поставок).

Для критически важных товаров или продуктов налоговый орган может потребовать включить в смарт-контракт некоторую идентификационную информацию о продуктах, подлежащих транзакции. Это могут быть серийные номера, защищенные идентификационные идентификаторы или тому подобное. Это позволяет полностью отслеживать эти критически важные товары, чтобы бороться с подделками.

На фиг. 8 представлен схематический чертеж иллюстративного выполнения электронного устройства 800, которое может использоваться, например, в качестве электронного устройства Алисы, Боба или Кэрол в способе или системе согласно настоящему изобретению.

Как проиллюстрировано на фиг. 8, электронное устройство 800 содержит блок вычисления, который может включать шину 805, блок 803 обработки, главное запоминающее устройство 807, ROM 808, устройство 809 для хранения, устройство 802 для ввода, устройство 804 для вывода и интерфейс 806 связи. Шина 805 может включать путь, который обеспечивает возможность связи между компонентами электронного устройства 800.

Блок 803 обработки может включать процессор, микропроцессор или логическую схему обработки информации, которые могут толковать и выполнять команды. Главное запоминающее устройство 807 может включать RAM или динамичное устройство для хранения другого типа, которые могут хранить информацию и команды для выполнения блоком 803 обработки. ROM 808 может включать устройство ROM или статичное устройство для хранения другого типа, которые могут хранить статичную информацию и команды для использования блоком 803 обработки. Устройство 809 для хранения может включать магнитный и/или оптический носитель записи и соответствующий ему драйвер.

Устройство 802 для ввода может включать механизм, который позволяет оператору вводить информацию в блок 803 обработки, такой как беспроводная клавишная панель, клавиатура, мышь, ручка, механизмы для распознавания голоса и/или биометрические механизмы и т. д. Устройство 804 для вывода может включать механизм, который выводит информацию оператору, включая дисплей, принтер, динамик и т.д. Интерфейс 806 связи может включать любой подобный приемопередатчику механизм, который позволяет электронному устройству 800 осуществлять связь с другими устройствами и/или системами (с такими как базовая станция, точка доступа WLAN и т.д.). Например, интерфейс 806 связи может включать механизмы для осуществления связи с другими устройством или системой через сеть.

Электронное устройство 800 может выполнять определенные операции или процессы, описанные в данном документе. Эти операции могут быть выполнены в ответ на блок 803 обработки, выполняющий команды программного обеспечения, содержащиеся на машиночитаемом носителе, таком как главное запоминающее устройство 807, ROM 808 и/или устройство 809 для хранения. Машиночитаемый носитель может быть определен как физическое или логическое запоминающее устройство. Например, логическое запоминающее устройство может включать область памяти в одном физическом запоминающем устройстве или область, распределенную между несколькими физическими запоминающими устройствами. Каждое из главного запоминающего устройства 807, ROM 808 и устройства 809 для хранения может включать машиночитаемые носители. Магнитные и/или оптические носители записи (например, считываемые CD-диски или DVD-диски) устройства 809 для хранения могут также включать машиночитаемые носители. Команды программного обеспечения могут быть считаны в главное запоминающее устройство 807 с другого машиночитаемого носителя, такого как устройство 809 для хранения, или с другого устройства через интерфейс 806 связи.

Команды программного обеспечения, содержащиеся в главном запоминающем устройстве 809, могут обеспечить осуществление блоком 803 обработки операций или процессов, описанных в данном документе, таких как, например, расшифрование машиночитаемого кода. В качестве альтернативы, аппаратная схема может быть использована вместо или в сочетании с командами программного обеспечения для выполнения процессов и/или операций, описанных в данном документе. Таким образом, описанные в данном документе реализации не ограничиваются какой-либо конкретной комбинацией аппаратного и программного обеспечения.

Любой из вышеупомянутых элементов может быть реализован в аппаратном обеспечении, про-

граммном обеспечении, программируемой пользователем вентильной матрице (FPGA), интегральной схеме специального назначения (ASIC), программно-аппаратном обеспечении или т.п.

Хотя изобретение было описано на основе подробных примеров, при этом подробные примеры служат исключительно для того, чтобы обеспечить специалисту в данной области техники лучшее понимание, и они не предназначены для ограничения объема изобретения. Объем изобретения значительно определяется прилагаемой формулой изобретения.

Сокращения

ASIC - интегральная схема специального назначения;

FPGA - программируемая пользователем вентильная матрица;

GST - налог на товары и услуги;

kA - ключ Алисы;

kB - ключ Боба;

kC - ключ Кэрол;

TR - запись транзакции;

VAT - налог на добавленную стоимость.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ регистрации в базе данных транзакции между первой стороной, далее называемой как "Алиса", и второй стороной, далее называемой как "Боб", и получения разрешения от третьей стороны, далее называемой как "Кэрол", на осуществление действия в отношении транзакции, при этом каждая из сторон Алиса, Боб и Кэрол имеет электронное устройство, выполненное с возможностью осуществления связи с базой данных посредством сети связи и выполненное с возможностью электронного подписывания данных, подлежащих отправке посредством сети связи, отличающийся тем, что способ включает

обеспечение электронным устройством Алисы создания записи, далее называемой как "запись транзакции", включающей

идентификатор, далее называемый как "идентификатор транзакции", для идентификации транзакции,

идентификатор для идентификации Алисы,

идентификатор для идентификации Боба, и

информацию, далее называемую как "информация о содержимом транзакции", относящуюся по меньшей мере к одному из типа транзакции и ценности, которую, как полагают, имеет транзакция;

электронное подписывание (s4) электронным устройством Алисы записи транзакции, при этом полученная в результате запись транзакции далее называется как "TR_{kA}";

регистрацию (s6) TR_{kA} в базе данных;

отправку уведомления (s8) на электронное устройство Кэрол о регистрации TR_{kA} в базе данных; и

определение (s10) того, что TR_{kA} соответствует правилу или набору правил и была электронно подписана электронным устройством Алисы;

электронное подписывание (s12) электронным устройством Кэрол TR_{kA}, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1}$";

регистрацию (s14) $TR_{kA,kC1}$ в базе данных;

отправку уведомления (s16) на электронное устройство Боба о регистрации $TR_{kA,kC1}$ в базе данных;

электронное подписывание (s18) электронным устройством Боба $TR_{kA,kC1}$, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1,kB}$";

регистрацию (s20) $TR_{kA,kC1,kB}$ в базе данных;

отправку уведомления (s22) на электронное устройство Кэрол о регистрации $TR_{kA,kC1,kB}$ в базе данных, и

определение (s24) того, что $TR_{kA,kC1,kB}$ была электронно подписана электронным устройством Боба;

электронное подписывание (s26) электронным устройством Кэрол $TR_{kA,kC1,kB}$, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1,kB,kC2}$";

регистрацию (s28) $TR_{kA,kC1,kB,kC2}$ в базе данных; и

обеспечение электронным устройством Кэрол осуществления действия (s30), где действие основано на информации о содержимом транзакции,

при этом при электронном подписывании (s12) TR_{kA} электронным устройством Кэрол со счета, связанного с Алисой, списывают сумму, которая считается результатом транзакции; и

при определении (s24) того, что $TR_{kA,kC1,kB}$ была электронно подписана электронным устройством Боба, счет, связанный с Бобом, пополняют на эту сумму.

2. Способ по п.1, отличающийся тем, что определение (s10) того, что TR_{kA} соответствует правилу или набору правил, включает верификацию электронным устройством Кэрол на основе идентификатора для идентификации Алисы, идентификатора для идентификации Боба и информации о содержимом транзакции соответствия транзакции правилу или набору правил.

3. Способ по п.1 или 2, отличающийся тем, что запись транзакции дополнительно включает параметр состояния, указывающий по меньшей мере на одно из того:

что запись транзакции была электронно подписана (s4) электронным устройством Алисы;

что TR_{kA} была зарегистрирована (s6) в базе данных;

что электронное устройство Кэрол получило уведомление (s8) о регистрации TR_{kA} в базе данных;

что TR_{kA} была определена (s10) как соответствующая правилу или набору правил и электронно подписанная электронным устройством Алисы;

что TR_{kA} была электронно подписана (s12) электронным устройством Кэрол;

что $TR_{kA,kC1}$ была зарегистрирована (s14) в базе данных;

что электронное устройство Боба получило уведомление (s16) о регистрации $TR_{kA,kC1}$ в базе данных;

что $TR_{kA,kC1}$ была электронно подписана (s18) электронным устройством Боба;

что $TR_{kA,kC1,kB}$ была зарегистрирована (s20) в базе данных;

что электронное устройство Кэрол получило уведомление (s22) о регистрации $TR_{kA,kC1,kB}$ в базе данных; и

что $TR_{kA,kC1,kB}$ была определена (s24) как электронно подписанная электронным устройством Боба;

что $TR_{kA,kC1,kB}$ была электронно подписана (s26) электронным устройством Кэрол;

что $TR_{kA,kC1,kB,kC2}$ была зарегистрирована (s28) в базе данных; и

что было обеспечено осуществление (s30) действия.

4. Способ по любому из предыдущих пунктов, отличающийся тем, что транзакция относится к объекту и объект маркируют кодом, представляющим собой или соответствующим идентификатору транзакции.

5. Способ по п.4, отличающийся тем, что он дополнительно включает маркировку объекта кодом после создания (s2) записи транзакции.

6. Способ по п.4 или 5, отличающийся тем, что он дополнительно включает

считывание (s32a) кода, нанесенного на объект; и

определение (s34a) путем запроса к базе данных по меньшей мере одного из того:

осуществлено ли действие для транзакции, идентифицируемой идентификатором транзакции, представленным или соответствующим считанному коду; и

совпадает ли тип объекта с информацией о содержимом транзакции, идентифицируемой идентификатором транзакции, представленным или соответствующим считанному коду.

7. Способ по любому из пп.1-3, отличающийся тем, что транзакция относится к услуге, и документ, связанный с услугой, маркируют кодом, представляющим собой или соответствующим идентификатору транзакции.

8. Способ по п.7, отличающийся тем, что он дополнительно включает маркировку документа кодом после создания (s2) записи транзакции.

9. Способ по п.7 или 8, отличающийся тем, что он дополнительно включает

считывание (s32b) кода, нанесенного на документ, связанный с услугой; и

определение (s34b) путем запроса к базе данных по меньшей мере одного из того:

осуществлено ли действие для транзакции, идентифицируемой идентификатором транзакции, представленным или соответствующим считанному коду; и

совпадает ли тип объекта с информацией о содержимом транзакции, идентифицируемой идентификатором транзакции, представленным или соответствующим считанному коду.

10. Способ по любому из пп.1-3, отличающийся тем, что транзакция относится к объекту и идентификатор транзакции соответствует подписи, далее называемой как "подпись объекта", генерируемой на основе по меньшей мере одного из:

свойства объекта; и

свойства защитного элемента на основе материала, наносимого на или прикрепляемого к объекту.

11. Способ по п.10, отличающийся тем, что он дополнительно включает

получение (s32c) подписи объекта; и

определение (s34c) путем запроса к базе данных по меньшей мере одного из того:

осуществлено ли действие для транзакции, идентифицируемой идентификатором транзакции, соответствующим полученной подписи объекта; и

совпадает ли тип объекта с информацией о содержимом транзакции, идентифицируемой идентификатором транзакции, соответствующим полученной подписи объекта.

12. Способ по любому из пп.1-3, отличающийся тем, что транзакция относится к услуге, и идентификатор транзакции соответствует подписи, далее называемой как "подпись документа, связанного с услугой", генерируемой на основании по меньшей мере одного из:

свойства документа, связанного с услугой; и

свойства защитного элемента на основе материала, наносимого на или прикрепляемого к документу, связанному с услугой.

13. Способ по п.12, отличающийся тем, что он дополнительно включает

получение (s32d) подписи документа, связанного с услугой; и

определение (s34d) путем запроса к базе данных по меньшей мере одного из того:

осуществлено ли действие для транзакции, идентифицируемой идентификатором транзакции, соот-

ветствующим полученной подписи документа, связанного с услугой; и

совпадает ли тип объекта с информацией о содержимом транзакции, идентифицируемой идентификатором транзакции, соответствующим полученной подписи документа, связанного с услугой.

14. Система регистрации в базе данных транзакции между первой стороной, далее называемой как "Алиса", и второй стороной, далее называемой как "Боб", и получения разрешения от третьей стороны, далее называемой как "Кэрол", на осуществление действия в отношении транзакции, при этом каждая из сторон Алиса, Боб и Кэрол имеет электронное устройство, выполненное с возможностью осуществления связи с базой данных посредством сети связи и выполненное с возможностью электронного подписывания данных, подлежащих отправке посредством сети связи, отличающаяся тем, что система выполнена с возможностью

обеспечения электронным устройством Алисы создания (s2) записи, далее называемой как "запись транзакции", включающей

идентификатор, далее называемый как "идентификатор транзакции", для идентификации транзакции,

идентификатор для идентификации Алисы,

идентификатор для идентификации Боба, и

информацию, далее называемую как "информация о содержимом транзакции", относящуюся по меньшей мере к одному из типа транзакции и ценности, которую, как полагают, имеет транзакция;

электронного подписывания (s4) электронным устройством Алисы записи транзакции, при этом полученная в результате запись транзакции далее называется как "TR_{kA}";

регистрации (s6) TR_{kA} в базе данных;

отправки уведомления (s8) на электронное устройство Кэрол о регистрации TR_{kA} в базе данных; и

определения (s10) того, что TR_{kA} соответствует правилу или набору правил и была электронно подписана электронным устройством Алисы;

электронного подписывания (s12) электронным устройством Кэрол TR_{kA}, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1}$";

регистрации (s14) $TR_{kA,kC1}$ в базе данных;

отправки уведомления (s16) на электронное устройство Боба о регистрации $TR_{kA,kC1}$ в базе данных;

электронного подписывания (s18) электронным устройством Боба $TR_{kA,kC1}$, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1,kB}$";

регистрации (s20) $TR_{kA,kC1,kB}$ в базе данных;

отправки уведомления (s22) на электронное устройство Кэрол о регистрации $TR_{kA,kC1,kB}$ в базе данных; и

определения (s24) того, что $TR_{kA,kC1,kB}$ была электронно подписана электронным устройством Боба;

электронного подписывания (s26) электронным устройством Кэрол $TR_{kA,kC1,kB}$, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1,kB,kC2}$";

регистрации (s28) $TR_{kA,kC1,kB,kC2}$ в базе данных; и

обеспечения электронным устройством Кэрол осуществления действия (s30), где действие основано на информации о содержимом транзакции,

при этом система выполнена с возможностью обеспечения того, что при электронном подписывании (s12) TR_{kA} электронным устройством Кэрол со счета, связанного с Алисой, списывают сумму, которая считается результатом транзакции; и

при определении (s24) того, что $TR_{kA,kC1,kB}$ была электронно подписана электронным устройством Боба, счет, связанный с Бобом, пополняют на эту сумму.

15. Электронное устройство для принятия участия в регистрации в базе данных транзакции между первой стороной, далее называемой как "Алиса", и второй стороной, далее называемой как "Боб", и для принятия участия в получении разрешения от третьей стороны, далее называемой как "Кэрол", на осуществление действия в отношении транзакции, при этом электронное устройство применимо как электронное устройство Кэрол, выполнено с возможностью осуществления связи с базой данных посредством сети связи и выполнено с возможностью электронного подписывания данных, подлежащих отправке посредством сети связи, отличающееся тем, что электронное устройство выполнено с возможностью

получения им уведомления (s8) о регистрации записи транзакции, далее называемой как "TR_{kA}", в базе данных, где TR_{kA} включает

идентификатор, далее называемый как "идентификатор транзакции", для идентификации транзакции,

идентификатор для идентификации Алисы, идентификатор для идентификации Боба, и

информацию, далее называемую как "информация о содержимом транзакции", относящуюся по меньшей мере к одному из типа транзакции и ценности, которую, как полагают, имеет транзакция, и

определения (s10) того, что TR_{kA} соответствует правилу или набору правил и была электронно подписана электронным устройством Алисы;

электронного подписывания (s12) электронным устройством Кэрол TR_{kA}, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1}$";

обеспечения регистрации (s14) $TR_{kA,kC1}$ в базе данных;

обеспечения отправки уведомления (s16) на электронное устройство Боба о регистрации $TR_{kA,kC1}$ в

базе данных;

последующего получения им уведомления (s22) о регистрации другой версии записи транзакции, при этом указанная версия далее называется как "$TR_{kA,kC1,kB}$", в базе данных, и

определения (s24) того, что $TR_{kA,kC1,kB}$ была электронно подписана электронным устройством Боба;

электронного подписывания (s26) электронным устройством Кэрол $TR_{kA,kC1,kB}$, при этом полученная в результате запись транзакции далее называется как "$TR_{kA,kC1,kB,kC2}$";

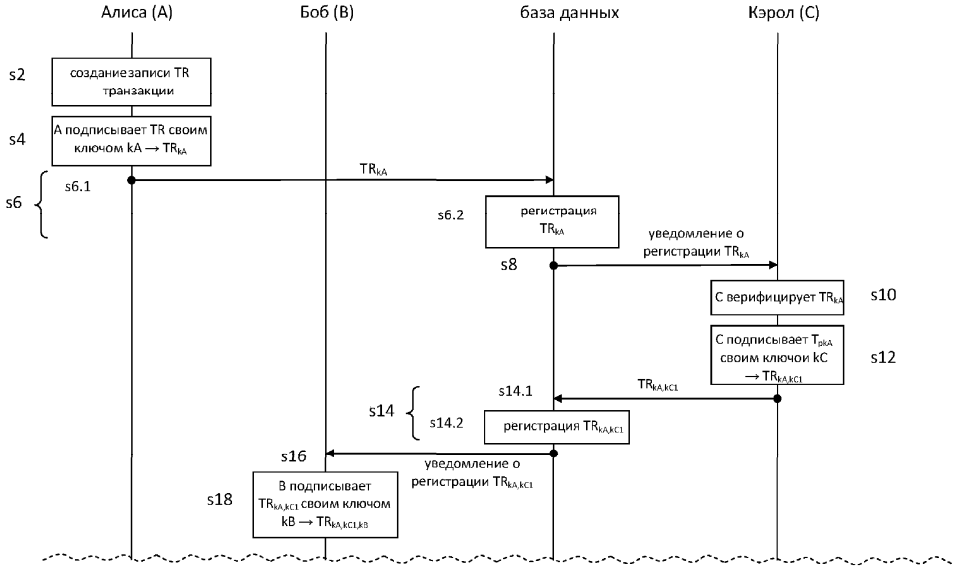
обеспечения регистрации (s28) $TR_{kA,kC1,kB,kC2}$ в базе данных; и

обеспечения осуществления действия (s30), где действие основано на информации о содержимом транзакции,

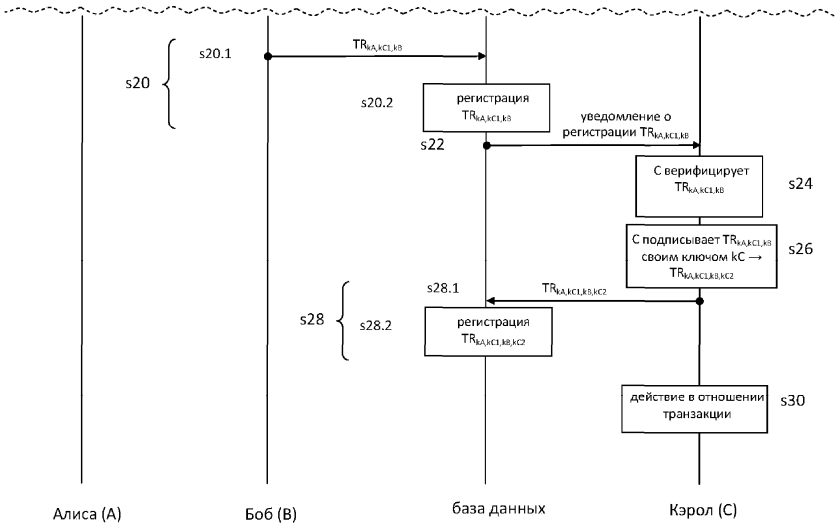
при этом электронное устройство выполнено с возможностью обеспечения того, что при электронном подписывании (s12) TR_{kA} электронным устройством Кэрол со счета, связанного с Алисой, списывают сумму, которая считается результатом транзакции; и

при определении (s24) того, что $TR_{kA,kC1,kB}$ была электронно подписана электронным устройством Боба, счет, связанный с Бобом, пополняют на эту сумму.

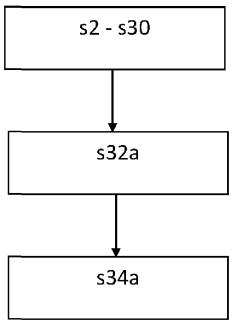
16. Машиночитаемый носитель, на котором хранятся машиночитаемые команды, обеспечивающие, при их выполнении на электронном устройстве или наборе электронных устройств, осуществление электронным устройством или набором электронных устройств способа по любому из пп.1-13.



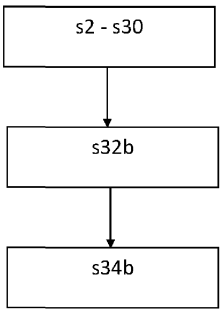
Фиг. 1a



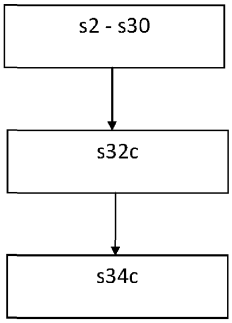
Фиг. 1b



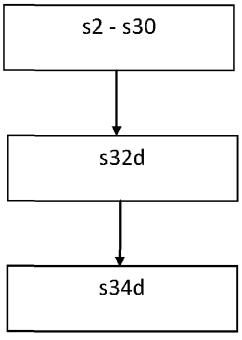
Фиг. 2



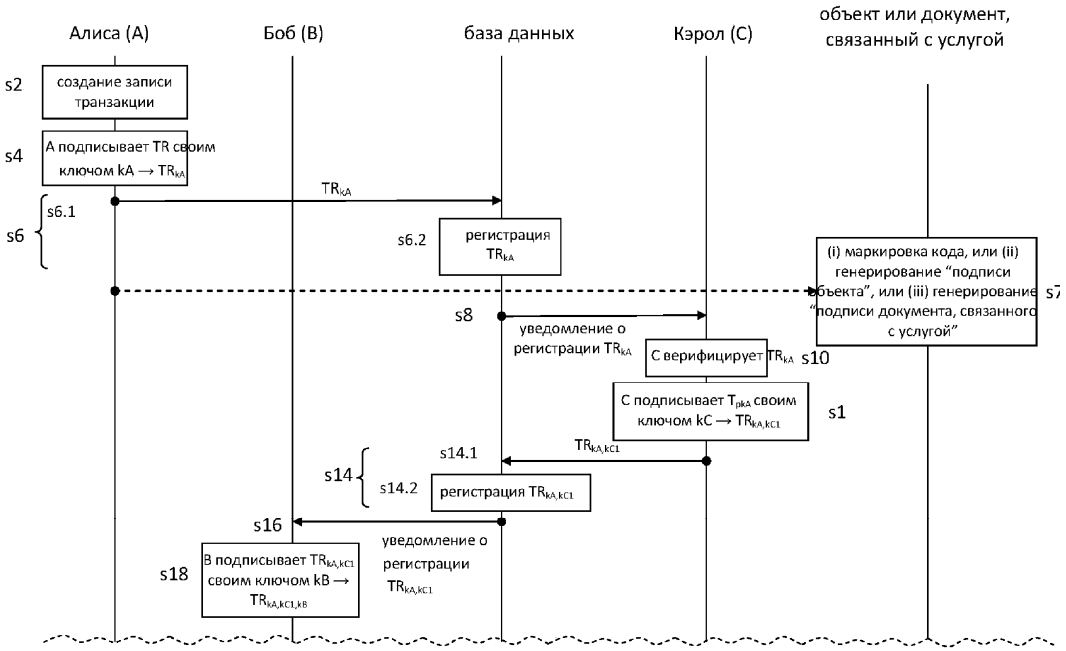
Фиг. 3



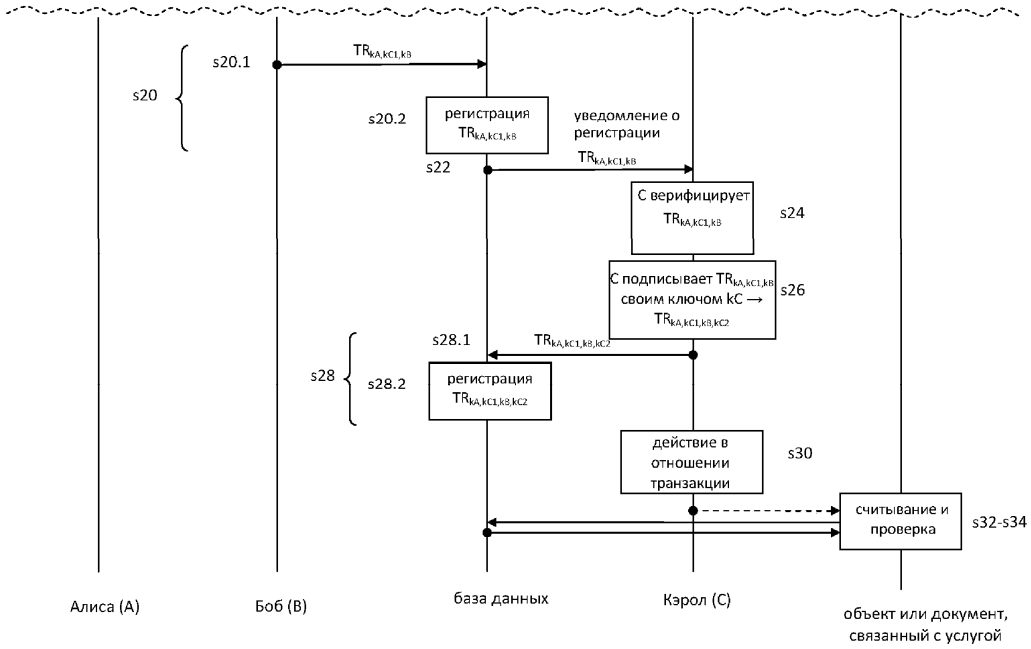
Фиг. 4



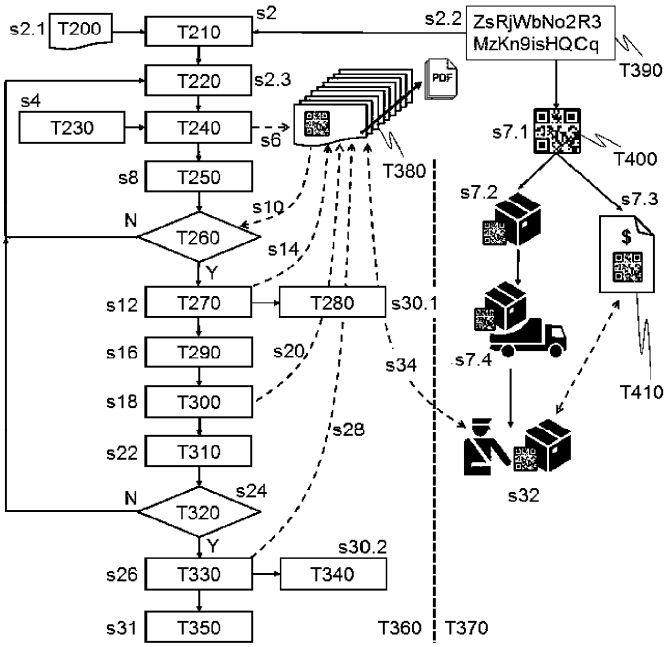
Фиг. 5


Алиса (A)
Боб (B)
база данных
Кэрол (C)
объект или документ, связанный с услугой
s2
создание записи транзакции
s4
A подписывает TR своим ключом kA → TR_kA
TR_kA
s6.1
s6
s6.2
регистрация TR_kA
(i) маркировка кода, или (ii) генерирование "подписи объекта", или (iii) генерирование "подписи документа, связанного с услугой"
s7
s8
уведомление о регистрации TR_kA
C верифицирует TR_kA
s10
C подписывает T_pkA своим ключом kC → TR_kA,kC1
s1
TR_kA,kC1
s14.1
s14
s14.2
регистрация TR_kA,kC1
s16
уведомление о регистрации TR_kA,kC1
s18
B подписывает TR_kA,kC1 своим ключом kB → TR_kA,kC1,kB

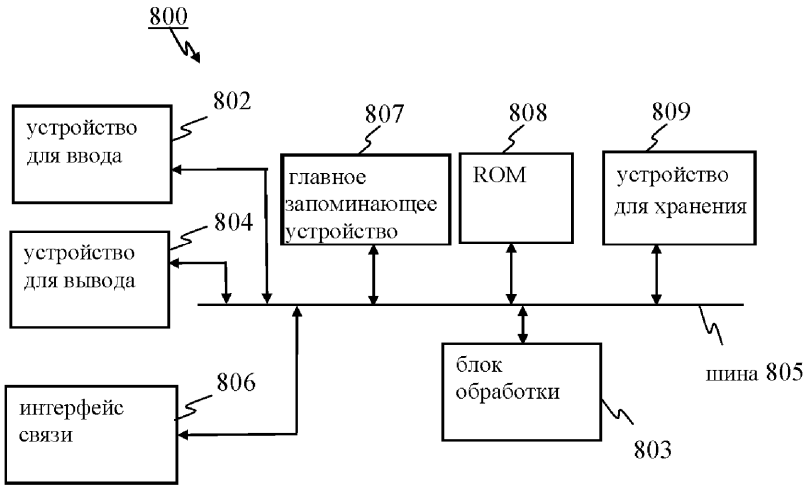
Фиг. 6a


s20.1
TR_kA,kC1,kB
s20
s20.2
регистрация TR_kA,kC1,kB
уведомление о регистрации
TR_kA,kC1,kB
s22
C верифицирует TR_kA,kC1,kB
s24
C подписывает TR_kA,kC1,kB своим ключом kC → TR_kA,kC1,kB,kC2
s26
s28.1
TR_kA,kC1,kB,kC2
s28
s28.2
регистрация TR_kA,kC1,kB,kC2
действие в отношении транзакции
s30
считывание и проверка
s32-s34
Алиса (A)
Боб (B)
база данных
Кэрол (C)
объект или документ, связанный с услугой

Фиг. 6b


s2.1
T200
T210
s2
s2.2
ZsRjWbNo2R3
MzKn9isHQCq
T390
T220
s2.3
s4
T230
T240
s6
T380
s7.1
T400
s8
T250
s10
s7.2
s7.3
N
T260
s14
Y
s12
T270
T280
s30.1
s16
T290
s20
s34
s7.4
T410
s18
T300
s28
s22
T310
N
s24
T320
s32
Y
s30.2
s26
T330
T340
s31
T350
T360
T370

Фиг. 7


800
802
807
808
809
устройство для ввода
главное запоминающее устройство
ROM
устройство для хранения
804
устройство для вывода
шина 805
806
блок обработки
интерфейс связи
803

Фиг. 8