(19) Евразийское патентное ведомство

(11) 034354 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.01.30

(21) Номер заявки
201891795

(22) Дата подачи заявки
2017.02.07

(51) Int. Cl. ***H04L 9/28*** (2006.01)

(54) СИСТЕМА И СПОСОБ ПРОВЕРКИ ПОДЛИННОСТИ ИНФОРМАЦИИ ДОКУМЕНТА

(31) **2016900405**
(32) **2016.02.08**
(33) **AU**
(43) **2019.01.31**
(86) **PCT/AU2017/050096**
(87) **WO 2017/136879 2017.08.17**

(71)(72)(73) Заявитель, изобретатель и патентовладелец:
МОЛОНИ ЛИНДСИ; СКОТТ ГАЙ (AU)

(74) Представитель:
Нагорных И.М. (RU)

(56) US-A1-20110161674
"What is proof of existence?" [retrieved from internet on 20 April 2016] <URL: https://web.archive.org/web/20151222163927/https://proofofexistence.com/about> published on 22 December 2015 as per Wayback Machine Entire document (see particularly paragraphs 1-3; sections "Common uses", "Technical foundations")
CROSBY, M. et al., "BlockChain Technology Beyond Bitcoin", Pantas and Ting, Sutardja Center for Entrepreneurship & Technology Technical Report, Berkeley Engineering, 16 October 2015, pages 1-35 Entire document (see particularly figures 2-15)
US-A1-20140254796
US-A1-20040103023
US-A1-20060271787

(57) В документе представлена система и способ для проверки подлинности информации документа для вариантов применения, включающих проверку подлинности информации документов сертификатов об окончании курсов, выданных зарегистрированными учебными организациями, проверку проездных документов и других важных документов, требующих проверки подлинности, таких как документы, выданные юридическими фирмами, бухгалтерскими фирмами, государственными учреждениями и т.п. Способ может включать этап создания записи о проверке, включающий прием метаданных содержимого документа из документа; генерирование хеша метаданных, используя метаданные содержимого документа; создание блокчейн-транзакции, содержащей хеш метаданных; и генерирование читаемых компьютером данных, кодирующих хеш метаданных; обновление документа читаемыми компьютером данными; и этап проверки документа, включающий прием документа; извлечение хеша метаданных из читаемых компьютером данных; и идентификацию хеша метаданных в блокчейн-транзакциях блокчейна для проверки подлинности метаданных документа.

034354 B1

034354 B1

Область техники

Изобретение относится к проверке подлинности информации документа и, в частности, но не обязательно полностью, к системе и способу проверки подлинности информации документа для вариантов применения, включающих проверку подлинности информации документации о присвоении квалификации, выданной зарегистрированными учебными организациями, проверку проездных документов и других важных документов, требующих проверку подлинности, таких как документы, выданные юридическими фирмами, бухгалтерскими фирмами, государственными учреждениями и т.п. Кроме того, технологии проверки подлинности, описанные в настоящем документе, могут широко применяться для различных форматов документов, включая печатный (т.е. бумажный проездной документ, проездной документ на смарт-карте) и цифровой (т.е. электронные форматы, включая формат PDF, включая хранящийся в репозиториях документов) форматы.

Уровень техники и краткое описание изобретения

Проверка подлинности документов желательна для вариантов применения, включающих, например, проверку подлинности информации в юридической документации, документации для удостоверения личности, документации по аккредитации, документации на допуск и т.д.

Проблемы с этими документами заключаются в том, что информация, содержащаяся в них, может изменяться, при этом, например, ложно заявляются аккредитации, происходит подделка документов и т.д.

D1: B US 2011/0161674 A1 (MING) от 30 июня 2011 г. предпринята попытка решения этой проблемы за счет раскрытия способа генерирования самоудостоверяющего документа, причем информация для установления подлинности документа закодирована в штрих-коде, который напечатан на документе. Хеш вычисляют из информации для установления подлинности и передают на сервер для хранения. При установлении подлинности сканированной копии документа штрих-код считывают для извлечения информации для установления подлинности. Целевой хеш вычисляют из извлеченной информации и передают на сервер для проверки. Сервер сравнивает целевой хеш с ранее сохраненным хешем. Если они не идентичны, то штрих-код был изменен. Если они идентичны, извлеченную информацию для установления подлинности используют для установления подлинности сканированной копии. Идентификатор документа может быть сгенерирован и передан на сервер, и использован сервером для индексации или поиска сохраненного хеша.

Однако документ D1 имеет указанный недостаток, и то что сервер может быть взломан, а хранящийся в нем хеш может быть изменен для соответствия подделанному документу. Поэтому документ D1 не подходит для вариантов применения, требующих высокой степени защиты, таких как использование для посадочных талонов, документов для установления личности и т.д.

Поэтому в предпочтительном варианте реализации настоящего изобретения используют распределенный основанный на криптографии блокчейн для хранения записей о проверке документов таким способом, что он не может быть изменен.

Далее, D2 "What is proof of existence?" [скачано из интернета 20 апреля 2016 г.] <URL: https://web.archive.org/web/20151222163927/https://proofofexistence.com/about> опубликовано 22 декабря 2015 г. от Wayback Machine раскрывает блокчейн для хранения распределённого онлайн доказательства существования документов посредством хранения отдельных криптографических дайджестов соответствующих документов в блокчейне.

В D2 хешируют электронный документ (такой как PDF) и сохраняют хеш в виде специальной биткойн-транзакции, которая кодирует/содержит хеш, посредством скрипта OP_RETURN. Он представляет собой биткойновый скриптовый операционный код, который маркирует результат транзакции как доказуемо не расходуемый и обеспечивает возможность вставки небольшого количества данных, которые в этом случае представляют собой хеш документа, а также маркера для идентификации всех транзакций из D2.

Однако D2 не направлен на проблему проверки подлинности информации в документе, а скорее на подтверждение того, что конкретный документ существовал в конкретном электронном формате в конкретный момент времени. Поэтому, D2 не может быть использован для обнаружения того, был ли документ подделан.

Кроме того, в D2 хешируют весь файл электронного документа, и поэтому он не может быть использован для печатных документов, где небольшие искажения внешнего вида при печати, сканировании, фотокопировании будут создавать полностью другой хеш при использовании системы из D2, и поэтому информация из документа, содержащаяся в нем, будет недоступной для проверки.

Поэтому в предпочтительном варианте реализации настоящего изобретения используют метаданные содержимого документа (хранящиеся при помощи хеша метаданных, в отличие от хеша документа из D1) в качестве основы для проверки и поэтому они могут быть использованы для печатных документов.

Кроме того, в D1 и D2 имеют недостаток в том, что информация в документе не может обновляться при сохранении пригодности для проверки документа.

Например, используя D2, для исходного документа будет создана первая биткойн-транзакция, и,

если исходный документ был обновлен, для обновленного документа будет создана вторая биткойн-транзакция.

Однако используя D2, как исходный документ, так и измененный документ будут казаться валидными несмотря на то, что исходный документ был заменен.

В отличие от этого, в варианте реализации настоящего изобретения используют блокчейн-транзакции обновления для целей обновления полей содержимого документа; таким образом, во время этапа проверки документа блокчейн может быть проверен в обратном хронологическом порядке для обнаружения того, был ли документ (или конкретные поля информации содержимого документа) заменен.

Кроме того, как D1, так и D2 имеют недостаток в том, что проверка не может проходить в течение заранее определенного периода.

В отличие от этого, в настоящем изобретении, согласно варианту реализации, создают блокчейн-транзакции, устанавливающие срок валидности.

Кроме того, как D1, так и D2 имеют недостаток в том, что документ не может быть аннулирован.

В отличие от этого, в настоящем изобретении, согласно варианту реализации, используют блокчейн-транзакции аннулирующего типа так, что аннулирование подлинности документа может быть обнаружено транзакцией аннулирующего типа, следующей по времени за предыдущей транзакцией проверки.

Кроме того, D1 и D2 имеют не достаток в том, что проверенная информация не может быть отображена вместе с документом для визуального сравнения.

В отличие от этого, в настоящем изобретении, согласно варианту реализации, сохраняют метаданные, такие как читаемые компьютером данные (т.е. 2D штрих-код) в самом документе или в блокчейне так, что информация может быть последовательно извлечена и отображена пользователю.

Следует понимать, что, если в настоящем документе сделана ссылка на какую-либо информацию уровня техники, такая ссылка не представляет собой допущение, что информация образует часть общеизвестных знаний в данной области техники в Австралии или любой другой стране.

Поэтому с учетом вышеизложенного, согласно одному варианту реализации, представлен способ проверки подлинности информации документа, включающий: этап создания записи о проверке, включающий: прием метаданных содержимого документа из документа; генерирование хеша метаданных, используя метаданные содержимого документа; создание блокчейн-транзакции, содержащей хеш метаданных; и генерирование читаемых компьютером данных, кодирующих хеш метаданных; обновление документа читаемыми компьютером данными; этап проверки документа, включающий: прием документа; извлечение хеша метаданных из читаемых компьютером данных; и идентификацию хеша метаданных в блокчейн-транзакциях блокчейна для проверки подлинности метаданных документа.

Как можно понять, D1 или D2 не раскрывают создание хеша метаданных для информации документа, создание связанной блокчейн-транзакции и обновление документа читаемыми компьютером данными (т.е. 2D штрих-кодом) с хешем метаданных.

Читаемые компьютером данные могут представлять собой штрих-код. Штрих-код может быть двумерным штрих-кодом.

Этап создания записи о проверке может дополнительно содержать подписание документа закрытым ключом, связанным с сервером проверки документа.

Способ может дополнительно включать сохранение метаданных содержимого документа так, что этап проверки документа может дополнительно включать извлечение метаданных содержимого документа и отображение метаданных содержимого документа.

Сохранение метаданных содержимого документа может включать кодирование метаданных в читаемых компьютером данных.

Сохранение метаданных содержимого документа может включать кодирование метаданных в блокчейн-транзакции.

Этап создания записи о проверке может дополнительно включать идентификацию метаданных содержимого документа из документа. Идентификация метаданных содержимого документа может включать оптическое распознавание символов.

Идентификация метаданных содержимого документа может включать выполнение запросов строки для поиска в отношении текста, извлеченного при помощи оптического распознавания символов.

Идентификация метаданных содержимого документа может включать выделение текста по меньшей мере в одной определенной пользователем области документа.

Способ может дополнительно включать этап обновления содержимого документа, включающий: прием обновленных метаданных содержимого документа для документа; генерирование нового хеша метаданных при помощи обновленных метаданных документа; создание дополнительной блокчейн-транзакции, содержащей новый хеш метаданных.

Этап проверки документа может включать: идентификацию двух или более блокчейн-транзакции, связанных с документом.

Этап проверки документа может дополнительно включать идентификацию того, что метаданные содержимого документа могут быть заменены на обновленные метаданные содержимого документа.

Способ может дополнительно включать идентификацию того, что в документе может быть заменено.

Способ может дополнительно включать этап аннулирования проверки документа, включающий: создание блокчейн-транзакции аннулирования, так что на этапе проверки документа способ также может включать: идентификацию блокчейн-транзакции аннулирования, следующей по времени за блокчейн-транзакцией, для завершения неудачей проверки подлинности информации документа.

Блокчейн-транзакция также определяет срок валидности, так что на этапе проверки документа способ может дополнительно включать завершение неудачей проверки документа, если срок валидности истек.

Способ может дополнительно включать создание блокчейн-транзакции восстановления срока валидности, содержащей дополнительный срок валидности, так что на этапе проверки документа дополнительный срок валидности может быть использован при определении валидности документа. Согласно другому аспекту, может быть предоставлена система для проверки подлинности информации документа, содержащая: сервер проверки информации документа, содержащий: базу данных, содержащую: блокчейн хешей; и таблицу метаданных документа, хранящуюся в связи с блокчейном односторонних хешей; программные модули, содержащие: модуль создания документа и модуль проверки информации документа; клиентский терминал, находящийся в функциональной связи с сервером проверки информации документа, содержащий: считыватель читаемых компьютером данных; программное приложение, находящееся в функциональной связи со считывателем читаемых компьютером данных, при этом программное приложение содержит: модуль проверки информации документа; причем при использовании система может быть выполнена с возможностью осуществления этапа создания записи о проверке, на котором: модуль создания документа сервера проверки информации документа: принимает метаданные документа, находящиеся в связи с документом; принимает или генерирует односторонний хеш из метаданных документа при помощи алгоритма хеширования; создает запись в блокчейне односторонних хешей для одностороннего хеша; генерирует читаемые компьютером данные, содержащие по меньшей мере одно из метаданных документа и одностороннего хеша; и передает читаемые компьютером данные в модуль создания документа; и этапа проверки информации документа, на котором: модуль проверки информации документа клиентского терминала принимает читаемые компьютером данные из документа; меньшей мере одно из клиентского терминала и сервера проверки информации документа, идентифицирует по меньшей мере одно из метаданных документа и одностороннего хеша из читаемых компьютером данных, причем, если принимаются только метаданные документа, генерирует односторонний хеш при помощи алгоритма одностороннего хеширования; и модуль проверки информации документа сервера проверки информации документа проверяет документ путем сравнения одностороннего хеша с записью в блокчейне хешей для одностороннего хеша.

Система может дополнительно содержать сервер лица, выдающего документ, находящийся в функциональной связи с сервером проверки информации документа.

Сервер проверки информации документа может быть выполнен с возможностью приема метаданных документа от сервера лица, выдающего документ.

Этап проверки информации документа может дополнительно включать по меньшей мере одно из клиентского терминала и сервера проверки информации документа, передающие по меньшей мере одно из одностороннего хеша и метаданных документа на сервер лица, выдающего документ, для дополнительной проверки документа.

Сервер лица, выдающего документ, может содержать базу данных, содержащую по меньшей мере одно из данных хеша и метаданных, и при этом дополнительная проверка может включать создание перекрестной ссылки по меньшей мере на одно из данных хеша и метаданных в базе данных сервера лица, выдающего документ.

Модуль проверки информации документа сервера проверки информации документа, может быть дополнительно выполнен с возможностью передачи результата проверки на клиентский терминал.

Программное приложение клиентского терминала может быть дополнительно выполнено с возможностью генерирования графического интерфейса пользователя, и при этом графический интерфейс пользователя может быть выполнен с возможностью отображения результата проверки.

Графический интерфейс пользователя может быть дополнительно выполнен с возможностью отображения по меньшей мере поднабора метаданных документа.

Система может содержать множество серверов проверки информации документа, и при этом блокчейн может представлять собой распределенный блокчейн, распределенный по множеству серверов проверки информации документа.

Создание читаемых компьютером данных может включать создание оптических читаемых компьютером данных.

Читаемые компьютером данные могут представлять собой 2D штрих-код.

Система может дополнительно содержать вставку читаемых компьютером данных в документ.

Также раскрыты и другие аспекты настоящего изобретения.

Краткое описание чертежей

Несмотря на любые другие формы, которые могут входить в рамки объема настоящего изобретения, далее будут описаны предпочтительные варианты реализации настоящего изобретения лишь в качестве примера со ссылкой на прилагаемые чертежи, на которых

на фиг. 1 показана система для проверки подлинности информации документа, согласно варианту реализации настоящего раскрытия;

на фиг. 2 показан пример способа создания записей о проверке подлинности информации документа, согласно варианту реализации;

на фиг. 3 показан пример способа проверки подлинности документа при помощи записей о проверке подлинности формально созданного документа, согласно варианту реализации;

на фиг. 4 показан пример способа обновления информации документа, при этом по-прежнему имея возможность проверки подлинности обновленного документа, согласно варианту реализации;

на фиг. 5 показан пример способа аннулирования записей о подлинности конкретного документа, согласно варианту реализации; и

на фиг. 6 показан пример графического интерфейса пользователя, отображенного клиентским терминалом системы, при проверке документа, показанного на фиг. 1, согласно варианту реализации настоящего раскрытия.

Описание вариантов реализации

С целью улучшения понимания принципов согласно настоящему раскрытию далее будет сделана ссылка на варианты реализации, изображенные на чертежах, а для их описания будет использована специфическая терминология. Тем не менее, следует понимать, что нет цели ограничить этим объем данного раскрытия. Любые изменения и дальнейшие модификации представленных в данном документе признаков изобретения, а также любые дополнительные варианты применения принципов раскрытия, представленных в данном документе, к которым, как правило, может дойти специалист в данной области техники, располагающим настоящим раскрытием, следует рассматривать как входящие в объем настоящего раскрытия.

Перед раскрытием и описанием конструкций, систем и соответствующих способов, относящихся к системе для проверки подлинности информации документа, следует понимать, что настоящее раскрытие не ограничено конкретными конфигурациями, этапами способа и материалами, раскрытыми в настоящем документе, поскольку они могут в некоторой степени отличаться. Также следует понимать, что терминология, используемая в настоящем документе, использована лишь с целью описания конкретных вариантов реализации, а не предназначена для ограничения, поскольку объем настоящего раскрытия будет ограничен только формулой изобретения и ее эквивалентами. При описании и заявлении объекта настоящего раскрытия будет использована следующая терминология, согласно определениям, представленным ниже.

Следует отметить, что при использовании в описании и прилагаемой формуле изобретения формы единственного числа включают множественное число объекта, если в контексте явным образом не указано иное. Используемые в настоящем документе термины "содержащий", "включающий", "вмещающий", "характеризующийся" и их грамматические эквиваленты являются включающими или открытыми выражениями, которые не исключают дополнительные, не перечисленные элементы или этапы способа. Следует отметить, что в следующем описании подобными или одинаковыми номерами позиций в различных вариантах реализации обозначены одинаковые или подобные признаки.

Архитектура системы для проверки подлинности информации документа

Ссылаясь теперь на фиг. 1, показана система 1 для проверки подлинности информации документа.

Как станет ясно из последующего описания, система 1 выполнена с возможностью проверки подлинности документов, таких как бумажные и электронные документы, в частности информации, представленной такими документами, для уменьшения или устранения подделки документа, фальсификации квалификаций и т.п.

В примере представленной архитектуры система 1 содержит сервер 19 проверки документа. Как будет описано более подробно ниже, сервер 19 проверки документа сконфигурирован при помощи различных программных модулей для выполнения различных вычислительных задач по обработке, описанных в настоящем документе.

В вариантах реализации сервер 19 проверки документа может иметь вид физического (такого как смонтированный на стойке) компьютерного сервера, но в альтернативных вариантах реализации сервера он может принимать вид виртуального варианта сервера, такого который может быть реализован посредством Amazon Web Services (AWS).

Как будет описано более подробно ниже, в вариантах реализации сервер 19 проверки документа хранит копию журнала блокчейна, и поэтому процессы, описанные в настоящем документе, в сервере 19 проверки документа могут быть распределены между множеством серверов 19.

Более конкретно, сервер 19 проверки документа содержит процессор 31 для обработки цифровых данных. В функциональной связи с процессором 31 посредством системной шины 33 находится запоминающее устройство 29.

Запоминающее устройство 29 выполнено с возможностью хранения цифровых данных, включающих компьютерный программный код. Таким образом, при работе процессор 31 может извлекать и исполнять инструкции, хранящиеся в запоминающем устройстве 29, и сохранять результирующие данные такого исполнения в запоминающем устройстве 29.

Память 29 может иметь форму комбинации энергозависимой (ОЗУ) и энергонезависимой (НЖМД) памяти.

Для удобства иллюстрации, память 29 показана на фиг. 1 как сконфигурированная из множества программных модулей 15 и связанных данных в нейронной базе 20 данных.

Как можно увидеть, программные модули 15 могут содержать модуль 14 создания записей о проверке документа, которые затем могут быть проверены модулем 13 проверки таким способом, который описан более подробно ниже.

Кроме того, данные, показанные в базе данных, были показаны для удобства иллюстрации как содержащие метаданные 23 документа, а в вариантах реализации, в которых используется блокчейн, данные 26 блокчейна, содержащие множество хешей 21, 22 документов, представляют собой метаданные 23 различных проверенных документов.

Сервер 19 проверки документа дополнительно содержит интерфейс 30 ввода/вывода для связи с различными периферийными устройствами компьютера, в том числе периферийными устройствами интерфейса пользователя и подобными.

Интерфейс 30 ввода/вывода дополнительно может связываться с периферийными устройствами для хранения данных, такими как USB-устройства для хранения данных. Таким образом, модули 15 компьютерного программного кода могут храниться на читаемом компьютером носителе, который может быть загружен на сервер 19 проверки посредством интерфейса 30 ввода/вывода (или сетевого интерфейса 32) так, чтобы сконфигурировать сервер 19 проверки документа для выполнения конкретных вычислительных задач по обработке, описанных в настоящем документе.

Сервер 19 проверки документа дополнительно содержит сетевой интерфейс 32 для отправки и приема данных по компьютерной сети, изображенной в виде сети Интернет 34 в показанной системе 1. Таким образом, сервер 19 проверки документа может находиться в функциональной связи с другими вычислительными объектами, показанными на фиг. 1.

С этой целью, система 1 в вариантах реализации может дополнительно содержать сервер 16 лица, выдающего документ. В общем, сервер 16 лица, выдающего документ, используется лицом, учреждением, организацией, органом управления или подобными, выдающими важные документы, требующие проверки подлинности способом, описанным в настоящем документе.

С этой целью, лицо, выдающее документ может использовать сервер 16 лица, выдающего документ, для целей хранения метаданных 18 документа, составления и создания документов, хранения и передачи документов по сети Интернет 34 и подобного.

С этой целью, сервер 16 лица, выдающего документ, подобным образом может содержать программные модули 10, содержащие модуль 11 проверки и модуль 12 создания. Кроме того, сервер 16 лица, выдающего документ может дополнительно хранить метаданные 18 документа и связанные хеши 24.

Таким образом, в вариантах реализации сервер 16 лица, выдающего документ, может выполнять все задачи по проверке подлинности документов и данных такие, в которых, например, организация использует сервер 16 лица, выдающего документ, для выполнения проверки документов локализованным образом.

В альтернативных вариантах реализации лицо 16, выдающее документ, может использовать сервер 19 проверки документа (такой как API на основе подписки) для выполнения всех или по меньшей мере некоторых задач по проверке документов.

Система 1 дополнительно содержит клиентский терминал 25, находящийся в функциональной связи по меньшей мере с одним из сервера 16 лица, выдающего документ, и сервера 19 проверки документа через сеть Интернет 34. В целом, клиентский терминал 25 может быть использован для отображения информации, указывающей на подлинность документа. В одном варианте реализации клиентский терминал 25 может иметь вид персонального компьютерного устройства, такого как ноутбук, мобильное устройство связи (такое как смартфон, такой как iPhone от компании Apple или подобный), которое пользователь может использовать для проверки подлинности документа.

Как можно увидеть, клиентский терминал 25 может дополнительно содержать сетевой интерфейс 32 для связи через сеть Интернет 34. В варианте реализации, в котором клиентский терминал 25 имеет вид мобильного устройства 25 связи, сетевой интерфейс 32 может отправлять и принимать данные по сотовой сети, такой как 3-5G сотовой сети передачи данных.

Подобным образом клиентский терминал 25 содержит процессор 31 для обработки цифровых данных и запоминающее устройство 29, находящееся в функциональной связи с процессором 31 посредством системной шины 33. Память 29 клиентского терминала 25 может дополнительно содержать операционную систему 66, такую как операционные системы Apple OS или Android.

Кроме того, клиентский терминал 25 может дополнительно содержать интерфейс 30 ввода/вывода, который в показанных вариантах реализации может связываться со считывателем 8 читаемых компьюте-

ром данных. С этой целью и как будет описано более подробно ниже, считыватель 8 может считывать читаемые компьютером данные 27 из документа 2 для проверки, чтобы проверить подлинность документа.

В варианте реализации, в котором клиентский терминал 25 имеет вид мобильного устройства связи, считыватель 8 может принимать вид устройства для захвата изображения/камеры, находящегося в клиентском терминале 25, а читаемые компьютером данные 27 могут принимать вид двумерного (2D) штрих-кода (такого как код быстрого реагирования (QR)). Таким образом для проверки документа 2 пользователь будет получать изображение 2D штрих-кода, нанесенного на документ 2, чтобы позволить клиентскому терминалу 25 проверить его подлинность.

В вариантах реализации клиентский терминал 25 (имеющий вид мобильного устройства связи) сконфигурирован с помощью загруженного программного приложения "app" 9, которое может быть загружено для установки и выполнения клиентским терминалом 25, например, из магазина программных приложений такого как Apple App Store или подобного.

С этой целью программное приложение 9 может содержать различные подмодули/программные модули, в том числе модуль 6 проверки и модуль 7 графического интерфейса пользователя.

На фиг. 1 также показана система 1, содержащая документ 2, который проверяется системой 1. Как указано выше, документ 2 может иметь вид печатного и цифрового документов. В последнем случае цифровые документы (электронные, такие как в формате PDF) могут храниться в базе 34 данных документов. С этой целью, конкретные документы могут быть извлечены при помощи URL-ссылки и идентификатора документа или другого уникального идентификатора, такого как хеш документа.

Как показано, документ 2 может содержать содержимое 5 документа. Кроме того, документ 2 может содержать читаемые компьютером данные 27, которые, как указано выше, могут принимать вид 2D штрих-кода, включенного или напечатанного на документе 2. Таким образом, читаемые компьютером данные 27 могут быть считаны клиентским терминалом 25 (или другим вычислительным объектом через сеть Интернет 34) для проверки его подлинности.

В вариантах реализации читаемые компьютером данные 27 могут содержать идентификатор документа, хеш 4 метаданных документа или метаданные 3 документа или их комбинацию в зависимости от конкретного варианта применения.

Следует отметить, что архитектура компьютера, показанная на фиг. 1, приведена в качестве примера лишь в целях иллюстрации.

В частности, конкретная архитектура, показанная на фиг. 1, представлена для варианта применения, в котором сервер 19 проверки документа развернут для использования на основе подписки, так что различные лица, выдающие документ, пользователи и т.п. могут иметь выборочный доступ к веб-функциям, предусмотренным сервером 19 проверки документа для проверки документов.

Однако следует особо отметить, что конкретная архитектура может быть модифицирована, в то же время выполняя такие же задачи и функции по проверке подлинности документов в пределах целевого объема вариантов реализации, описанных в настоящем документе.

Пример способа 35 создания записи о подлинности документа

После представленного выше описания вычислительной архитектуры далее будут представлены различные примеры способов использования системы 1 для проверки подлинности документа, включая способ 35, показанный на фиг. 2, для создания записи о подлинности документа.

Способ 35 используют для создания записей о подлинности документа, которые могут быть использованы в дальнейшем, и последующих стадий проверки.

Следует отметить, что способ 35 представлен лишь в качестве примера, и что для всех вариантов реализации не следует применять какие-либо технические ограничения, соответственно.

На этапе 39 способа 35 получают содержимое документа. Если документ 2 представляет собой физический документ, документ может быть отсканирован, используя сканер, и содержимое документа может быть получено при помощи оптического распознавания символов (OPC). В качестве альтернативы, если документ 2 представляет собой цифровой документ, содержимое документа может быть считано из самого документа электронной файловой системы (например, путем считывания различных метаданных документа или содержимого документа, в том числе когда содержимое документа также может быть распознано при помощи OPC) или, в качестве альтернативы, извлечено из соответствующей базы данных, такой как база 17 данных сервера 16 лица, выдающего документ.

В целом, содержимое документа является важным содержимым документа (называемым в данном документе метаданными, которые хешированы в хеш метаданных, такой как хеш MD5, SHA256 или другой подходящий односторонний хеш), последующие изменения или модификации которого в этом важном содержимом документа могут быть обнаружены системой 1. В других вариантах реализации весь документ может быть хеширован в хеш документа, чтобы любые изменения документа могли быть обнаружены.

Также, как будет описано более подробно ниже, система 1 может иметь функцию обновления содержимого/метаданных документа или аннулирования аккредитации подлинности.

На этапе 40 могут быть идентифицированы различные метаданные. Как указано выше, метаданные

представляют собой важную информацию, содержащуюся в документе.

Например, для документа о присвоении квалификации метаданные могут представлять собой название выдавшей организации, имя получившего и наименование квалификации. В качестве дополнительного примера, для посадочного талона метаданные могут представлять собой имя пассажира, номер рейса, выход на посадку, номер паспорта, пункт назначения и т.п. В вариантах реализации система 1 выполнена с возможностью создания хеша 4 метаданных из метаданных, так что подделка важных метаданных может быть обнаружена системой 1. Кроме того, метаданные могут храниться в нехешированном формате (открытым текстом или зашифрованными), чтобы обеспечить последующее отображение клиентским терминалом 25 во время проверки.

Использование метаданных на этапе 40 (представляющих некоторую важную информацию документа) может быть полезным для печатных документов, так что важная информация, представленная в них, отделяется для проверки. Таким образом, документ может быть модифицирован другим образом, например, включая искажения при фотокопировании и сканировании, печати на различных печатных бланках или подобное, не влияя на возможность проверки его подлинности.

Однако, как указано выше, следует отметить, что в вариантах реализации, в частности для электронных документов, метаданные не обязательно должны быть отделены от документа вместо хеширования всего содержимого файла электронных данных. В частности, в этом варианте реализации, в отличие от хеширования метаданных, файл электронного документа может быть хешем, таким как хеш MD5, SHA256 или подобный. В вариантах реализации могут быть использованы отдельные хеш метаданных и хеш документа, так что модификация документа или важных метаданных в нем могут быть обнаружены независимо. В вариантах реализации используемые метаданные могут быть заданы пользователем. Например, некоторые метаданные, используемые из базы 29 данных лица, выдающего документ, задаются пользователем.

В альтернативных вариантах реализации, в которых метаданные извлекают из самого документа, могут быть заданы фильтры строки для поиска, чтобы позволить системе 1 извлечь (включая использование OPC) соответствующие метаданные.

Например, для документации о присвоении квалификации только название организации, лицо, получившее документ, и квалификация могут быть заданы как хранимые в качестве метаданных для целей проверки так, что другое содержимое документа может быть изменено без влияния на возможность проверки подлинности метаданных документа.

Таким образом, могут быть использованы различные строки для поиска, чтобы позволить системе 1 выделить эти поля метаданных.

Еще в одних вариантах реализации могут быть заданы области/прямоугольники в документе (представляющие положение метаданных документа в документе), чтобы позволить системе извлечь только текст из заданных областей.

На этапе 41 может быть получен или сгенерирован идентификатор документа. В предпочтительном варианте реализации идентификатор документа является глобально уникальным (GUID), чтобы предотвратить или по существу исключить конфликты идентификаторов документов.

Идентификатор документа может быть использован для уникальной идентификации документов для проверки. Например, идентификатор документа может быть использован для извлечения документов из базы 34 данных документов, используя URL, содержащий идентификатор документа. Кроме того, идентификатор документа может быть использован для обновления документов с целью аннулирования документов.

В вариантах реализации идентификатор документа может быть сгенерирован системой 1. Однако в альтернативных вариантах реализации идентификатор 1 документа может быть предоставлен лицом, выдающим документ, как, например, когда зарегистрированная учебная организация выдает документы о присвоении квалификации в порядке последовательных номеров.

В вариантах реализации идентификатор документа может быть дополнительно хеширован как часть хеша метаданных или хеша документа, чтобы предотвратить подделку идентификатора документа.

Однако следует отметить, что в некоторых вариантах реализации идентификатор документа не является обязательным условием. Например, печатная копия документа может содержать 2D штрих-код на ней, представляющий собой хеш метаданных, причем метаданные представляют собой информацию, отображенную документом. При этом 2D штрих-код может быть отсканирован для проверки содержимого документа без необходимости использования идентификатора документа.

В дополнительных вариантах реализации хеш, созданный из файла документа или метаданных, может служить в качестве уникального идентификатора документа.

На этапе 42 создают хеш 4. Предпочтительно, хеш представляет собой односторонний хеш, такой как MD5, SHA256 или подобные. Хеш обеспечивает возможность сжатия потенциально большого количества информации до небольшого размера, но, что важно, подделка даже одной буквы содержимого сильно влияет на хеш.

В предпочтительном варианте реализации хеш 4 представляет собой хеш метаданных, так что метаданные (важная информация документа) хешируются для обеспечения возможности обнаружения после-

дующего изменение этой важной информации в документе. Однако, как также упоминалось выше, в другом варианте реализации хеш 4 может быть хешем документа файла электронного документа.

Другая информация также может быть хеширована в хеше 4, включая идентификатор документа.

В варианте реализации комбинация вышеуказанной информации может быть хеширована для образования хеша 4.

В предпочтительном варианте реализации система 1 использует блокчейн для целей хранения хешей 4, чтобы иметь возможность обеспечить не изменяемый распределенный и достоверный журнал проверочных документов.

В частности, как показано на фиг. 1, сервер 19 проверки документа может хранить копию журнала 26 блокчейна в базе 20 данных, которая может быть синхронизирована с другим сервером 19 проверки документации.

При этом на этапе 43 хеш добавляется к блокчейн-транзакции, которую затем последовательно добывают и добавляют в блок в блокчейне. Существуют различные способы, которыми хеш может быть добавлен в блокчейн, включая, если используют блокчейн биткойна, в биткойновый скриптовый операционный код. В альтернативных вариантах реализации может быть использован модифицированный блокчейн, содержащий подходящие поля данных.

Соответственно, при проверке документа блокчейн может быть проверен, чтобы установить, находится ли хеш 4 (который может быть отсканирован с 2D штрих-кода 27 или, в качестве альтернативы, рассчитан в процессе обработки) в блокчейне.

В вариантах реализации поиск хеша может проводиться во всем блокчейне, но в предпочтительном варианте реализации может быть использован отдельный индекс хеша для ускорения процесса поиска хеша.

Следует отметить, что не во всех вариантах реализации обязательно использование блокчейна. Например, сервер 16 лица, выдающего документ, может хранить базу данных метаданных 18 документа (или содержимого документа) и связанных хешей 24 документа или идентификаторов документа для обеспечения возможности проверки документов отдельно без использования распределенного журнала. В этом случае система 1 все еще хранит копию метаданных 18 (чтобы, например, обеспечить отображение метаданных в процессе проверки для визуального сравнения пользователем) и связанных хешей, чтобы иметь возможность обнаружить подделку метаданных (хотя и без обеспечения защиты от подделки базы 17 данных, чего можно избежать, используя блокчейн).

На этапе 44 могут быть сгенерированы читаемые компьютером данные, которые в дальнейшем могут быть использованы вместе с документом для проверки.

На этапе 45 читаемые компьютером данные вставляют в документ видимым или невидимым образом.

В одном варианте реализации, упомянутом выше, читаемые компьютером данные 27 могут иметь вид 2D штрих-кода, содержащего одно или более из хеша документа, идентификатора документа и метаданных документа.

В предпочтительном варианте реализации читаемые компьютером данные 27 являются видимыми, чтобы обеспечить возможность печати, сканирования и фотокопирования документа.

Например, документ может быть модифицирован для видимого отображения читаемых компьютером данных 27, так что, например, PDF документ модифицируют для включения изображения 2D штрих-кода внизу с правой стороны документа. В этом случае при последующей проверке электронного документа или его печати пользователь может использовать камеру смартфона 25 для захвата изображения 2D штрих-кода для проверки содержимого или метаданных документа.

В альтернативных вариантах реализации для электронных документов, существующих только в электронном виде, читаемые компьютером данные 27 не обязательно должны быть видимы человеку и они могут быть включены, например, в метаданные документа. В этом случае при отображении документа программа отображения документа может в фоновом режиме проверять связанные метаданные, и отображать и указывать, проверен ли документ или нет. Например, PDF документ может быть обновлен, чтобы метаданные PDF документа содержали читаемые компьютером данные 27 (которые, как указано выше, могут включать одно или более из метаданных документа, идентификатора документа и хеша документа). В связи с этим, при отображении в приложении для PDF, таком как Adobe Acrobat reader, программное обеспечение для PDF может автоматически проверять читаемые компьютером данные 27 и отображать указание о том, проверен ли документ или нет.

В альтернативных вариантах реализации, например, при использовании для проездной документации и подобного, могут быть использованы RFID-метки. На этапе 46, на котором документ имеет вид электронного документа, документ может также быть подписан цифровой подписью, чтобы предотвратить подделку или модификацию читаемых компьютером данных, включенных или вставленных в него.

В одном варианте реализации сервер 19 проверки документа может подписывать документ, используя закрытый ключ, так что другие лица могут затем проверить, что сервер 19 проверки документа действительно подписал документ, используя связанный открытый ключ.

Пример способа 36 проверки подлинности документа

Далее переходя к фиг. 3 показан пример способа 36 проверки подлинности документа. Как будет очевидно из следующего описания, способ 36 используют для целей проверки подлинности документа, используя читаемые компьютером данные 27, связанные с ним.

Способ 36 начинается с этапа 47, на котором получают документ. Например, физический документ может быть получен на руки или, в качестве альтернативы, электронный документ может быть получен из файловой системы, загружен по URL или т.п.

На этапе 48 читаемые компьютером данные, связанные с документом, сканируют или считывают.

Для физического документа, содержащего читаемые компьютером данные 27 в виде 2D штрих-кода, штрих-код может быть считан, используя считыватель 8, находящийся в клиентском терминале 25.

Для электронного документа читаемые компьютером данные 27 могут быть извлечены при помощи программы отображения документа (такой как Adobe Acrobat).

На этапе 49 может быть извлечен хеш из читаемых компьютером данных 27.

Если читаемые компьютером данные содержат идентификатор документа, идентификатор документа также может быть получен из читаемых компьютером данных, чтобы иметь возможность сравнить с идентификатором документа, используемым для получения документа или связанного с документом.

На этапе 50, если система 1 использует блокчейн, блокчейн может быть проверен на блоки, содержащие транзакции, содержащие хеш и, в вариантах реализации, связанный идентификатор документа.

Если соответствующая транзакция будет найдена в блокчейне, на этапе 51 пользователю может быть отображена проверка, показывающая, что документ является подлинным.

Кроме того, на этапе 52 из читаемых компьютером данных могут быть извлечены метаданные, которые затем могут быть отображены клиентским терминалом 25, чтобы обеспечить пользователю возможность сравнения метаданных, извлеченных из читаемых компьютером данных, с теми, которые отображены на документе.

В некоторых других вариантах реализации метаданные 23 могут храниться в самом блокчейне 26, так что метаданные 23 могут быть получены из блокчейна 26 во время проверки, чтобы избежать необходимость хранения метаданных 23 в самом 2D штрих-коде 27.

Пример способа 37 обновления метаданных документа

Переходя к фиг. 4 показан пример способа 37 обновления метаданных документа.

В частности, в вариантах реализации может возникнуть необходимость в обновлении метаданных документа.

Например, в случае посадочных талонов может произойти изменение выхода. В качестве еще одного примера, в случае документа о присвоении квалификации может быть изменено имя получателя с девичьей фамилии.

В связи с этим, может быть использован способ 37 для обеспечения возможности обновления некоторых полей документа, в то же время сохраняя возможность проверки подлинности документа.

В связи с этим, на этапе 53 может быть сгенерирован или получен идентификатор документа для обновляемого документа (или другой уникальный идентификатор, такой как хеш документа или метаданных).

На этапе 54 получают обновленные метаданные (или содержимое документа). Например, обновленные метаданные могут содержать новую фамилию.

Обновленные метаданные (или обновленное содержимое документа) хешируют на этапе 55.

Далее, на этапе 56 добавляют новый хеш при помощи дополнительной транзакции в блокчейн.

На этапах 57-59 документ может быть модифицирован для включения новых читаемых компьютером данных 27. Однако обновление 2D штрих-кода 27 не обязательно имеет место, особенно для документов, которые уже были распространены.

В связи с этим, при последующей проверке документа блокчейн-транзакции могут быть проверены в обратном хронологическом порядке, причем самая поздняя по времени транзакция проверки используется в качестве текущей транзакции проверки.

В качестве альтернативы, если хеш будет извлечен из документа, связанного с блокчейн-транзакцией, для которого существует блокчейн-транзакция с более поздним временем, клиентский терминал 25 может проинформировать пользователя о том, что метаданные/содержимое документа устарело, и что документ был заменен.

В вариантах реализации результат проверки может показывать, что документ был заменен. Однако в других вариантах реализации результат проверки может показывать какие метаданные содержимого документа были заменены.

Например, при создании первой блокчейн-транзакции проверки идентификатор документа и исходный хеш метаданных могут храниться в блокчейне.

Затем при получении обновления для метаданных документа в блокчейне может быть создана новая блокчейн-транзакция, содержащая идентификатор документа и новый хеш метаданных (представляющий обновленные метаданные).

В связи с этим, при последующей проверке документа читаемые компьютером данные 27 могут

быть считаны клиентским терминалом 25 для извлечения идентификатора документа и хеша метаданных.

Затем в блокчейне может быть проведен поиск блокчейн-транзакции, связанных с идентификатором документа.

Однако если система 1 будет идентифицировать две или более транзакций, система 1 может сравнить полученный хеш с двумя или более транзакциями для определения того, является ли конкретная транзакция текущей или она была заменена.

Пример способа 38 аннулирования подлинности документа

Далее переходя к фиг. 5, показан пример способа 38 аннулирования подлинности документа.

Более конкретно, может возникнуть необходимость в аннулировании документа. Например, возможно, что по прошествии времени было обнаружено, что человек, получивший документ о присвоении квалификации, имеет квалификацию, полученную неправомерным путем, и поэтому документ о присвоении квалификации должен быть аннулирован.

Если используется технология блокчейна, невозможно удалить транзакцию из блокчейна.

В связи с этим, в способе 38 используют транзакцию аннулирования, которую добавляют в блокчейн для аннулирования документа.

Более конкретно, способ 38 начинается с этапа 60, на котором получают запрос на аннулирование для конкретного документа, идентифицированного идентификатором документа (или другим уникальным идентификатором, таким как хеш документа или метаданных).

На этапе 61 транзакцию аннулирования добавляют в блокчейн. Транзакцию аннулирования определяют по типу транзакции (типу транзакции аннулирования, который снова может храниться в биткойновом скриптовом операционном коде) и идентификатору документа.

В связи с этим, при последующей проверке на этапе 62 принимают читаемые компьютером данные для документа, и из них извлекают идентификатор документа и/или хеш документа.

На этапе 63 в блокчейне выполняют поиск совпадающих идентификаторов или хешей документа.

Однако для любых транзакций проверки, идентифицированных в блокчейне, на этапе 65 система 1 определяет последующую транзакцию аннулирования в блокчейне, связанную с идентификатором или хешем документа, и поэтому на этапе 64 проверка заканчивается неудачей.

Ограниченные периоды проверки подлинности

В вариантах реализации документы могут иметь ограниченную подлинность. Причем, например, документы валидны только в течение 12 месяцев, как это может быть в случае автомобильных прав.

В связи с этим, транзакция проверки, хранящаяся в блокчейне, может задавать срок валидности (который снова может храниться в биткойновом скриптовом операционном коде). В связи с этим во время проверки система 1 может проверять даты ввода транзакций проверки, и, если текущая дата превышает срок валидности, проверка заканчивается неудачей. Например, если система 1 идентифицирует транзакцию проверки в блокчейне как проведенную более чем 12 месяцев назад, но в то же время транзакция проверки определяет, что проверка валидна в течение периода, составляющего 12 месяцев, и система 1 не может идентифицировать какие-либо дополнительные последующие по времени транзакции проверки, связанные с документом, тогда проверка заканчивается неудачей.

Таким образом, срок валидности может быть обновлен посредством добавления следующих по времени транзакций проверки блокчейна.

Пример применения архитектуры системы 1 для проверки документов о присвоении квалификации, выданных зарегистрированными учебными организациями (ЗУО)

После приведенного выше описания архитектуры системы 1 и связанных методологий, далее будет описан пример применения системы 1 для использования при проверке документов о присвоении квалификации, выданных зарегистрированными учебными организациями (ЗУО).

Как можно увидеть, сервер 16 лица, выдающего документ (ЗУО), содержит множество программных модулей 10.

В вариантах реализации, описанных в данном документе, программные модули 10 могут содержать модуль 12 создания записи о проверке для целей создания записи документа для последующей проверки.

Как также можно увидеть, сервер 19 проверки информации документа сам по себе может содержать множество программных модулей 15, самих содержащих модуль 14 создания записи о проверке.

Кроме того, программные модули 10 сервера 16 лица, выдающего документ (ЗУО), могут дополнительно содержать модуль 11 проверки для последующей проверки документов.

Подобным образом, программные модули 15 сервера 19 проверки информации документа подобным образом содержат модуль 13 проверки для целей проверки документов, как будет описано более подробно ниже.

Как указано выше, такая функция проверки и создания может выполняться одними и теми же модулями, если функция сервера 16 лица, выдающего документ (ЗУО), и сервера 19 проверки информации документа реализована одним сервером.

В этом примерном варианте реализации человек по имени Джеймс Смит успешно закончил курс в конкретной ЗУО.

После завершения курса данные сертификата о присвоении квалификации или о курсе записываются ЗУО.

Более конкретно, как можно увидеть, сервер 16 лица, выдающего документ (ЗУО), содержит базу 17 данных.

Кроме того, база 17 данных может содержать метаданные 18 или другой тип структурированных данных, сконфигурированных для хранения различных информационных полей относительно курса, который прошел Джеймс Смит.

В связи с этим, в базе 17 данных может быть записана следующая информация:

a. Имя: Джеймс Смит.

b. Дата выдачи: 7 июля 2007 г.

c. Номер документа: 0007/07/2007.

d. Выдавшая ЗУО: Служба обучения Allwest.

e. Национальный код поставщика услуг №: 51925.

f. Тип сертификации: Сертификат о присвоении квалификации/курс.

g. Подписавшее должностное лицо: Боб Купер.

h. Должность подписавшего должностного лица: Руководитель.

Далее на этапе создания записи о проверке из вышеуказанных метаданных создают хеш. В одном варианте реализации метаданные конкатенируют в строку, содержащую:

a. Джеймс Смит|19051983|M|007 007 007|0007/07/2007|Служба обучения Allwest|51925|07072007|Сертификат о присвоении квалификации|Эксплуатация карьерных самосвалов|Боб Купер|Руководитель.

Затем конкатенированную строку хешируют при помощи алгоритма одностороннего хеширования, такого как MD5, SHA256 или другой алгоритм хеширования. Например, такой хеш может генерировать следующий хеш:

a. 25908e49524e4828190dae3d79b894eec7ec3e4843c8bca6ef9f384c679167bc.

Затем хеш метаданных сохраняют с тем, чтобы быть использованным для последующей проверки информации документа.

Более конкретно, как можно увидеть, сервер 19 проверки информации документа содержит базу 20 данных для хранения различной информации, включая данные хеша.

В связи с этим, вышеуказанный хеш метаданных вставляют в базу 20 данных. Такая вставка может включать прием сервером 19 проверки информации документа метаданных (или хеша метаданных) от базы 17 данных сервера 16 лица, выдающего документ (ЗУО), например, с постоянными интервалами, по запросу и т.п.

Следует отметить, что алгоритм хеширования, описанный в настоящем документе, может выполняться любым из вычислительных объектов, находящихся в целевом объеме вариантов реализации, описанных в настоящем документе. Другими словами, хеширование может быть выполнено, например, сервером 16 лица, выдающего документ (ЗУО), или сервером 19 проверки информации документа.

В предпочтительном варианте реализации для предотвращения мошенничества, возникающего при вставке сфальсифицированных хеширующих записей в базу 20 данных, система 1 может реализовывать распределенный блокчейн 26 публичных журналов, так что каждая запись хеша поддается проверке согласно другим записям хеша в базе 20 данных.

В вариантах реализации, описанных в настоящем документе, проверку проводит один сервер 19 проверки информации документа. Однако следует понимать, что блокчейн 26 может быть распределенным блокчейном, распределенным среди некоторого числа серверов 19.

Следует отметить, что любые распределенные блокчейны на основе криптографии могут быть использованы в целевом объеме вариантов реализации, описанных в настоящем документе, и включая те, которые используются в или подобны блокчейнам Bitcoin, ehterum, litecoin и подобным.

В этих вариантах реализации каждая ЗУО 16 ("лицо, выдающее информацию документа") и сервер 19 проверки документа могут быть определены как "адрес выдающего лица", который может быть адресом биткойн-кошелька. Емкость, транзакции в биткойн-блокчейне могут быть уникально связаны с соответствующим сервером 16 лица, выдающего документ, или сервером 19 проверки документа.

В вариантах реализации метаданные могут также храниться в базе 20 данных сервера 19 проверки информации документа. Таким образом, имея хеш (или идентификатор документа), можно искать метаданные.

В этом варианте реализации хеш может служить в качестве первичного ключа. Однако следует понимать, что база 20 данных не обязательно должна содержать метаданные 23, чтобы содержать только хеш для целей проверки информации документа.

Далее генерируют читаемые компьютером данные, содержащие по меньшей мере одно из хеша и метаданных. Создание читаемых компьютером данных будет обеспечивать возможность вставки читаемых компьютером данных в документ, такой как сертификат о присвоении квалификации, являющийся печатным или электронным (т.е. PDF) документом, который затем может быть прочитан при помощи клиентского терминала 25 для целей проверки подлинности документа и метаданных документа, храня-

щихся в нем.

В предпочтительном варианте реализации читаемые компьютером данные реализованы в виде 2D штрих-кода. Например, при создании 2-D штрих-кода из читаемых компьютером данных для кодирования данных могут быть использованы следующие форматы:

a. [Хеш_ключа] || [Имя] || [Дата рождения в формате ДД/ММ/ГГГГ] || [Пол] || [Номер водительских прав] || [Номер документа] || [Выдающая ЗУО] || [Национальный код поставщика №] || [Дата выдачи в формате ДД/ММ/ГГГГ] || [Тип сертификата] || [Тип лицензии] || [Подписавшее должностное лицо] || [Должность подписавшего должностного лица]

Таким образом, при помощи подходящего алгоритма может быть создан следующий 2-D штрих-код:

Создав читаемые компьютером данные, их затем вставляют в или печатают на документе.

Как можно увидеть на фиг. 1, показан документ 2, являющийся сертификатом о присвоении квалификации для курса, законченного Джеймсом Смитом. В этом конкретном варианте реализации документ 2 выдан как PDF документ сервером 16 лица, выдающего документ (ЗУО). В связи с этим Джеймс Смит может использовать электронный PDF документ 2 в качестве доказательства его квалификации для различных целей, связанных с трудоустройством.

Как можно увидеть, документ может содержать содержимое 5 документа, которое может содержать обычную читаемую человеком информацию, включая по меньшей мере поднабор вышеописанных метаданных. Однако, как указано выше, в решениях уровня техники документ может быть отредактирован или в электронном виде, или в физическом, чтобы представить ложную информацию. В связи с этим, документ, за счет дополнительного содержания читаемых компьютером данных 27, может быть проверен при помощи клиентского терминала 25. Как можно увидеть, читаемые компьютером данные 27, содержащиеся в документе 2, могут содержать по меньшей мере одно из метаданных 3, хеша 4 метаданных или документа и идентификатора документа.

В вариантах реализации только метаданные 3 могут быть закодированы в читаемых компьютером данных 27, так что хеш может быть вычислен из метаданных для проверки. В других вариантах реализации в читаемых компьютером данных 27 закодирован только хеш 4, так что метаданные могут быть получены из базы 20 данных сервера 19 проверки информации документа, или базы 17 данных сервера 16 лица, выдающего документ (ЗУО), или блокчейна. Как можно увидеть, клиентский терминал 25 содержит программное приложение 9, выполненное с возможностью реализации признаков и функций, описанных в настоящем документе. Как указано выше, в варианте реализации клиентский терминал 25 представляет собой мобильное устройство связи, такое как смартфон или подобное. Здесь клиентский терминал 25 может содержать считыватель 8, который в вариантах реализации может иметь вид камеры мобильного телефона.

При использовании клиентский терминал 25 может загружать программное приложение 9 для выполнения клиентским терминалом 25, например, из магазина приложений, такого как Apple iTunes store или подобного.

Как можно увидеть, программное приложение 9 может содержать модуль 6 проверки, выполненный с возможностью осуществления выполняемой клиентским терминалом функции для проверки информации документа, а также модуль 7 графического интерфейса пользователя (ГИП), представляющий собой графический интерфейс пользователя, предназначенный для отображения различной информации пользователю клиентского терминала. В связи с этим, для проверки подлинности документа пользователь клиентского терминала, используя считыватель 8, будет сканировать читаемые компьютером данные 27 в виде 2-D штрих-кода, обеспеченного на документе. По меньшей мере одно из клиентского терминала 25 и сервера 19 проверки информации документа выполнено с возможностью идентификации по меньшей мере одного из метаданных 3 и хеша 4 после получения читаемых компьютером данных из документа 2.

В предпочтительном варианте реализации метаданные 3 закодированы в читаемых компьютером данных 27, так что ГИП 7 клиентского терминала 25 может отображать метаданные.

Еще в одном предпочтительном варианте реализации как хеш 4, так и метаданные 3 закодированы в читаемых компьютером данных 27, так что клиентский терминал 25 может генерировать хеш при помо-

щи алгоритма хеширования, используя закодированные метаданные 3, чтобы проверить по меньшей мере то, что закодированный хеш 4 соответствует метаданным 3. В вариантах реализации может быть использован проприетарный алгоритм хеширования, чтобы предотвратить незаконное генерирование и кодирование хеша мошенниками, использующими известный алгоритм хеширования.

Кроме того, клиентский терминал 25, находящийся в функциональной связи с сервером 19 проверки информации документ посредством сети передачи данных, такой как сеть Интернет, выполнен с возможностью передачи по меньшей мере одного из метаданных 3 и хеша 4 на сервер 19 проверки информации документа для проверки.

Сервер 19 проверки информации документа выполнен с возможностью сравнения хеша, полученного от клиентского терминала 25 (или вычисленного из метаданных 3, считанных клиентским терминалом 25), со значением хеша, хранящимся в блокчейне 26.

Если выявлено совпадение, сервер 19 проверки информации документа может направить результат проверки назад на клиентский терминал 25, подтверждая, что информация документа является подлинной.

В качестве альтернативы, если совпадение не было выявлено, сервер 19 проверки выполнен с возможностью передачи результата неудачной проверки назад на клиентский терминал 25, показывая, что информация документа может быть сфальсифицированной или была подделана.

В любом случае ГИП 7 выполнен с возможностью отображения результатов проверки пользователю клиентского терминала. Кроме того, ГИП 7 может отображать связанные метаданные.

Например, и переходя далее к фиг. 6, показан пример интерфейса 28, отображаемого на ГИП 7, где документ был проверен. Как можно увидеть, интерфейс 28 содержит различные метаданные и подтверждение того, что информация документа является подлинной.

В вариантах реализации система 1 выполнена с возможностью осуществления дополнительной проверки, при которой записи, сохраненные в базе 17 данных сервера ЗУО, дополнительно образованы с перекрестными ссылками (в случае, когда записи были обновлены или аннулированы). В частности, перекрестные ссылки могут быть выполнены при помощи по меньшей мере одного из хеша и метаданных. Как можно увидеть, в варианте реализации база 17 данных сервера 16 лица, выдающего документ (ЗУО), может быть выполнена с возможностью хранения значений 24 хеша в связи с метаданными 19. Как указано выше, такие значения 24 хеша могут быть получены от сервера 19 проверки информации документа или, в качестве альтернативы, вычислены самим сервером 16 лица, выдающего документ (ЗУО). Как также упоминалось выше, в вариантах реализации база 17 данных не обязательно содержит значения 24 хеша, когда метаданные 18 образованы с перекрестными ссылками. Когда метаданные 18 образованы с перекрестными ссылками, по меньшей мере одно из клиентского терминала 25 и сервера 19 проверки информации документа может направлять дополнительный запрос модулю 11 проверки сервера 16 лица, выдающего документ (ЗУО), для проверки данных, хранящихся в базе 17 данных. Например, клиентский терминал 25 может передавать номер документа на сервер 16 ЗУО для проверки того, что номер документа является подлинным. Могут быть сделаны другие перекрестные ссылки, входящие в целевой объем вариантов реализации, описанных в настоящем документе.

Пример применения системы 1 для печатной документации

Далее будет описан пример применения системы 1 для печатной документации.

Более конкретно, как указано выше, проблемы печатной документации могут включать то, что внешний вид документации изменяется со временем, что вызвано, например, искажениями фотокопирования и тому подобным. В связи с этим, в данном примере применения будет описана система 1, которая выполнена с возможностью проверки печатного документа, несмотря на изменения внешнего вида.

Более конкретно, в данном примере печатный документ представляет собой договор купли-продажи, который был подписан продавцом, покупателем и свидетелем. В печатном документе также определена недвижимость, подлежащая продаже, которая идентифицирована номером лота. В связи с этим, для целей создания записей о проверке документа оформленный документ договора может быть отсканирован при помощи сканера, и при этом система 1 затем выполняет распознавание документа при помощи OPC для идентификации соответствующих метаданных из договора купли-продажи. В этом примере соответствующие метаданные представляют собой имена продавца и покупателя, а также номер лота.

С этой целью, система 1 выполнена с возможностью извлечения таких метаданных из документа. Например, используя OPC, система 1 может быть выполнена с возможностью использования сравнения строк или подобного для извлечения этих полей из данных.

В качестве альтернативы, на клиентском терминале 25 может быть отображено отсканированное изображение документа, так что юрист может выделить метаданные, которые необходимо проверить, например, при помощи растягивания прямоугольников вокруг связанного текста, используя мышь.

Кроме того, юристом может быть задан идентификатор документа, который является созданным файловой системой идентификатором документа.

Получив соответствующие метаданные, система 1 хеширует метаданные (и идентификатор документа в вариантах реализации) и создает транзакцию проверки в блокчейне.

Кроме того, система 1 создает читаемые компьютером данные в виде 2D штрих-кода, который затем печатают на документе договора купли-продажи.

2D штрих-код содержит хеш 4 метаданных, идентификатор документа и метаданные.

Договор купли-продажи затем фотокопируют, а фотокопию затем направляют юристу, занимающемуся операциями по передаче недвижимости.

Однако в процессе фотокопирования возникают небольшие визуальные искажения.

Тем не менее, для проверки договора купли-продажи юрист, занимающийся операциями по передаче недвижимости, захватывает изображение документа, используя камеру своего мобильного устройства 25 связи.

Мобильное устройство 25 связи содержит программное приложение 9, которое идентифицирует 2D штрих-код и извлекает хеш метаданных, идентификатор документа и метаданные из 2D штрих-кода.

Мобильное устройство 25 связи затем передает запрос на проверку по сети Интернет 34 на сервер 19 проверки документа. Запрос на проверку содержит хеш, но в вариантах реализации может дополнительно включать идентификатор документа.

Сервер 19 проверки документа затем выполняет поиск по транзакциям проверки блокчейна и идентифицирует ранее созданную транзакцию проверки.

Сервер 19 проверки документа затем передает ответ о проверке на мобильное устройство 25 связи, так что мобильное устройство 25 связи может отобразить указание на то, что запись о проверке существует.

Далее, в одном варианте реализации мобильное устройство 25 связи юриста, занимающегося операциями по передаче недвижимости, может отображать метаданные, извлеченные из 2D штрих-кода. В связи с этим, юрист, занимающийся операциями по передаче недвижимости, может визуально проверить имена сторон и номер лота на документе, отображенные мобильным устройством 25 связи, чтобы убедиться в их соответствии.

Следует отметить, что клиентский терминал 25 может повторно хешировать метаданные, хранящиеся в 2D штрих-коде, чтобы подтвердить, совпадает ли созданный хеш с хешем 2D штрих-кода (чтобы предотвратить подделку метаданных в штрих-коде).

В качестве альтернативы, во время исходной транзакции проверки метаданные могут также храниться в блокчейне, так что метаданные могут быть переданы на клиентский терминал 25 с сервера 19 проверки документа для отображения.

В альтернативных вариантах реализации, в отличие от отображения полей метаданных для визуального сравнения юристом, занимающимся операциями по передаче недвижимости, мобильное устройство связи может выполнять оптическое распознавание символом для того, чтобы считать текст с документа (несмотря на искажения фотокопирования) и подтвердить, совпадает ли распознанный текст с метаданными.

Например, для метаданных, хранящихся в 2D штрих-коде или блокчейне, клиентский терминал 25 может выполнять поиск по OPC тексту для идентификации таких метаданных. Если они не идентифицированы, например, если сканированный документ не содержит такой же номер лота, тогда проверка заканчивается неудачей.

В вариантах реализации релевантные метаданные выделены в пределах границ, которые, например, в варианте реализации, описанном выше, юрист рисует прямоугольники вокруг метаданных, отображенных на экране, которые необходимо проверить. Например, номер лота может находиться в центре посередине сверху страницы, тогда как имена сторон могут быть снизу в правом и левом углах документа, соответственно.

В связи с этим, при проверке мобильное устройство 25 связи выполнено с возможностью распознавания текста только в обозначенных границах, а затем сравнения текста, извлеченного из этих обозначенных границ, с метаданными.

При использовании камеры мобильное устройство 25 связи может определять углы страницы для ориентации, чтобы иметь возможность точно разместить обозначенные границы.

Пример применения архитектуры системы 1 для проверки посадочных талонов

Далее будет описан пример применения системы для проверки посадочных талонов.

В частности, имеют место проблемы с существующими системами посадочных талонов, заключающиеся в том, что данные, напечатанные на них, могут быть подделаны. Кроме того, записи в базе данных могут быть изменены для совпадения с поддельной печатью, так что при регистрации сотрудники аэропорта могут не заметить посадочный талон, который был подделан для совпадения с измененной записью в базе данных.

Таким образом, в этом варианте реализации при изначальной печати посадочных талонов система обработки записей пассажиров направляет соответствующие метаданные на сервер 19 проверки документа.

В этом варианте реализации релевантные метаданные могут включать идентификатор посадочного талона, имя пассажира и выход на посадку.

Сервер 19 проверки документа может хешировать метаданные и создавать запись в блокчейне, и

направлять 2D штрих-код в систему обработки записей пассажиров, который затем печатают на посадочном талоне.

Далее, перед отправлением перенос полета может приводить к обновлению номера выхода. В связи с этим, система обработки записей пассажиров идентифицирует всех релевантных пассажиров и для этих идентифицированных релевантных пассажиров направляет уведомление об обновлении на сервер 19 проверки документа.

Например, для каждого посадочного талона система обработки записей пассажиров может передавать идентификатор посадочного талона и обновленный номер выхода.

Для каждого обновления сервер 19 проверки документа создает новую запись в блокчейне.

Далее, при регистрации 2D штрих-коды посадочных талонов сканируют и из штрих-кодов извлекают идентификатор посадочного талона и метаданные (имя пассажира и номер выхода). В итоге такая информация также может быть получена при помощи OPC с печати на посадочном талоне.

Такие извлеченные метаданные затем могут быть переданы на сервер 19 проверки документа для проверки.

В вариантах реализации компьютер выхода на посадку может хранить копию блокчейна, чтобы избежать времязатратных запросов по сети Интернет серверу 19 проверки документа.

Далее, предполагая, что была попытка замены пассажира другим именем, посадочный талон может быть подделан для замены имени, напечатанном на посадочном талоне, а также связанной записи в базе данных системы обработки записей пассажиров. Метаданные, хранящиеся в 2D штрих-коде, могли быть дополнительно модифицированы.

Однако для такой модификации имени проверка сервером 19 проверки документа закончится неудачей, поскольку сервер 19 проверки документа не будет находить совпадение хеша нового имени и хеша, хранящегося в блокчейне.

Далее, для обновленного номера выхода на посадочном талоне может все еще быть представлен старый номер выхода.

В связи с этим, хеш, закодированный в 2D штрих-коде, будет устаревшим (поскольку он все еще представляет старый номер выхода).

Однако при регистрации новый номер выхода может быть направлен компьютером проверки пассажиров на сервер 19 проверки документа, причем сервер 19 проверки документа может идентифицировать дополнительную транзакцию проверки относительно идентификатора посадочного талона с новым номером выхода и, таким образом, пройти проверку посадочного талона. В этом отношении следует отметить, что проверка закончится неудачей для любого другого представленного номера выхода, не совпадающего с транзакцией обновления выхода в блокчейне.

Толкование

Беспроводной.

Настоящее изобретение может быть реализовано при помощи устройств, согласующихся с другими сетевыми стандартами и для других приложений, включая, например, другие WLAN стандарты и другие беспроводные стандарты. Приложения, которые могут быть использованы, включают IEEE 802.11 беспроводные LAN и соединения, а также беспроводную сеть Ethernet. В контексте настоящего документа термин "беспроводной" и его производные могут быть использованы для описания схем, устройств, систем, способов, технологий, каналов связи и т.д., которые могут передавать данные посредством использования модулированного электромагнитного излучения через не твердотельную среду. Термин не подразумевает, что связанные устройства не содержат никаких проводов, хотя в некоторых вариантах реализации они могут не содержать их. В контексте настоящего документа термин "проводной" и его производные могут быть использованы для описания схем, устройств, систем, способов, технологий, каналов связи и т.д., которые могут передавать данные посредством использования модулированного электромагнитного излучения через твердотельную среду. Термин не подразумевает, что связанные устройства соединены электропроводными проводами.

Процессы.

Если явным образом не указано иное, как видно из следующего описания, следует понимать, что по всему описанию, использование терминов, таких как "обработка", "вычисление", "расчет", "определение", "анализ" или подобные, относится к действию и/или процессам компьютера или вычислительной системы, или аналогичного электронного вычислительного устройства, которое манипулирует и/или преобразует данные, представленные как физические, такие как электронные, величины, в другие данные, подобным образом представленные как физические величины.

Процессор.

Подобным образом, термин "процессор" может относиться к любому устройству или части устройства, которая обрабатывает электронные данные, например, из регистров и/или памяти, для преобразования этих электронных данных в другие электронные данные, которые, например, могут храниться в регистрах и/или памяти. "Компьютер" или "вычислительное устройство", или "вычислительная машина", или "вычислительная платформа" могут содержать один или более процессоров.

Методологии, описанные в настоящем документе, в одном варианте реализации могут выполняться

одним или более процессорами, которые принимают читаемый компьютером (также называемый машиночитаемым) код, содержащий набор инструкций, которые при выполнении одним или более процессорами выполняют по меньшей мере один из способов, описанных в данном документе. Подразумевается любой процессор, способный выполнять набор инструкций (последовательных или иных), который определяет действия, подлежащие выполнению. Таким образом, один пример представляет собой типичную систему обработки данных, которая содержит один или более процессоров. Система обработки данных также может содержать подсистему памяти, включая основную ОЗУ, и/или статическую ОЗУ, и/или ПЗУ.

Читаемый компьютером носитель.

Кроме того, читаемое компьютером несущее средство может образовывать или может быть включено в компьютерный программный продукт. Компьютерный программный продукт может храниться на используемом компьютером несущем средстве, причем компьютерный программный продукт содержит читаемое компьютером программное средство для побуждения процессора выполнять способ, описанный в настоящем документе.

Соединенные в сеть или множественные процессоры.

В альтернативных вариантах реализации один или более процессоров работают как отдельное устройство или могут быть соединены, например, по сети с другим(и) процессором(ами), в сетевую группу, один или более процессоров могут работать в качестве сервера или клиентского устройства в сетевой среде сервер-клиент, или в качестве пиринговой машины в пиринговой или распределенной сетевой среде. Один или более процессоров могут образовывать сетевое устройство, сетевой маршрутизатор, коммутатор или мост, или любую машину, способную выполнять набор инструкций (последовательных или иных), который определяет действия, подлежащие выполнению машиной. Следует отметить, что хотя на некоторой(ых) схеме(ах) показан только один процессор и одна память, которая хранит читаемый компьютером код, специалистам в данной области техники будет ясно, что многие компоненты, описанные выше, включены, но явным образом не показаны или не описаны, чтобы не затруднять понимание аспекта изобретения. Например, несмотря на то, что показана только одна машина, термин "машина" следует также понимать, как включающий любой набор машин, которые отдельно или совместно выполняют набор (или множество наборов) инструкций для выполнения любой одной или нескольких методологий, описанных в настоящем документе.

Дополнительные варианты реализации.

Таким образом, один вариант реализации каждого из способов, описанных в данном документе, представлен в виде читаемого компьютером несущего средства, несущего набор инструкций, например, компьютерную программу, которая предназначена для выполнения на одном или более процессорах. Таким образом, как будет понятно специалистам в данной области техники, варианты реализации настоящего изобретения могут быть воплощены как способ, устройство, такое как устройство специального назначения, устройство, такое как система обработки данных, или читаемое компьютером несущее средство. Читаемое компьютером несущее средство несет читаемый компьютером код, содержащий набор инструкций, который при выполнении на одном или более процессорах побуждает процессор или процессоры выполнять способ. Следовательно, аспекты настоящего изобретения могут принимать вид способа, полностью аппаратного варианта реализации, полностью программного варианта реализации или варианта реализации, объединяющего программные и аппаратные аспекты. Кроме того, настоящее изобретение может принимать вид несущего средства (например, компьютерный программный продукт на читаемом компьютером средстве хранения), несущего читаемый компьютером программный код, находящийся в этом средстве.

Несущее средство.

Программное обеспечение также может быть передано или принято по сети посредством устройства сетевого интерфейса. Хотя несущее средство показано в примерном варианте реализации как одно средство, термин "несущее средство" следует рассматривать как включающий одно средство или множество средств (например, централизованная или распределенная база данных и/или связанные кэши и серверы), которые хранят один или более наборов инструкций. Термин "несущее средство" также следует рассматривать как включающий любое средство, который может хранить, кодировать или переносить набор инструкций для выполнения одним или более процессорами, и который побуждает один или более процессоров выполнять любую одну или более методологий настоящего изобретения. Несущее средство может иметь множество форм, включая, но не ограничиваясь, энергонезависимые средства, энергозависимые средства и среды передачи данных.

Реализация.

Следует понимать, что этапы описанных способов выполняются в одном варианте реализации соответствующим процессором (или процессорами) системы обработки данных (т.е. компьютерной), выполняющей инструкции (читаемый компьютером код), хранящиеся в памяти. Следует также понимать, что настоящее изобретение не ограничено какой-либо конкретной реализацией или технологией программирования, и что настоящее изобретение может быть реализовано при помощи любых подходящих технологий для реализации функционала, описанного в данном документе. Настоящее изобретение не ограни-

чено каким-либо конкретным языком программирования или операционной системой.

Средства для выполнения способа или функции.

Кроме того, некоторые из вариантов реализации описаны в данном документе как способ или комбинация элементов способа, которые могут выполняться процессором процессорного устройства, компьютерной системой или другими средствами выполнения функции. Таким образом, процессор с необходимыми инструкциями для выполнения такого способа или элемента способа образует средство для выполнения способа или элемента способа. Кроме того, элемент описанного в настоящем документе варианта реализации устройства является примером средства для выполнения функции, выполняемой элементом для цели реализации настоящего изобретения.

Соединенный.

Подобным образом, следует отметить, что термин "соединенный" при использовании в формуле изобретения не следует толковать как ограниченный только прямыми соединениями. Таким образом, объем выражения "устройство A, соединенное с устройством B" не должен ограничиваться устройствами или системами, где выход устройства A непосредственными соединен со входом устройства B. Это означает, что существует путь между выходом A и входом B, который может быть путем, содержащим другие устройства или средства. "Соединенный" может означать, что два или более элементов находятся в непосредственном физическом или электрическом контакте, или что два или более элементов находятся в непрямом контакте друг с другом, но все еще совместно работают или взаимодействуют друг с другом.

Варианты реализации.

Ссылка во всем описании на "один вариант реализации" или "вариант реализации" означает, что конкретный признак, структура или характеристика, описанные в отношении варианта реализации, включены по меньшей мере в один вариант реализации настоящего изобретения. Таким образом, упоминание фраз "в одном варианте реализации" или "в варианте реализации" в различных местах в настоящем описании не обязательно все относятся к одному и тому же варианту реализации, но могут относиться к нему. Кроме того, конкретные признаки, структуры или характеристики могут быть объединены любым подходящим образом, что должно быть очевидно специалисту в данной области из данного раскрытия, в одном или более вариантах реализации. Подобным образом, следует понимать, что в вышеуказанном описании примеров вариантов реализации настоящего изобретения различные признаки настоящего изобретения иногда сгруппированы вместе в одном варианте реализации, на фигуре или в их описании для целей упрощения раскрытия и помощи в понимании одного или более различных аспектов настоящего изобретения. Данный метод раскрытия, однако, не следует толковать как отражающий намерение, заключающееся в том, что заявленное изобретение требует больше признаков, чем это явно указано в каждом пункте формулы изобретения. Скорее, как отражено в нижеследующей формуле изобретения, аспекты изобретения заключаются в меньшем количестве признаков, чем все признаки одного вышеизложенного варианта реализации. Таким образом, формула изобретения, следующая за подробным описанием конкретных вариантов реализации, настоящим явным образом включена в это подробное описание конкретных вариантов реализации, при этом каждый пункт формулы сам по себе является отдельным вариантом реализации настоящего изобретения. Кроме того, хотя некоторые варианты реализации, описанные в данном документе, включают некоторые, а не другие признаки, включенные в другие варианты реализации, комбинации признаков из различных вариантов реализации предполагаются включенными в объем настоящего изобретения и образуют другие варианты реализации, что должно понятно специалистам в данной области техники. Например, в нижеследующей формуле изобретения любые из заявленных вариантов реализации могут быть использованы в любой комбинации.

Различные примеры объектов.

При использовании в данном документе, если не указано иное, использование порядковых прилагательных "первый", "второй", "третий" и т.д., для описания общего объекта показывают только, что ссылаются на различные случаи подобных объектов, и они не предназначены для обозначения того, что объекты, описанные таким образом, должны быть представлены в изложенной последовательности как во времени, так и в пространстве, по категории, или любым другим образом.

Конкретные детали.

В описании, представленном в настоящем документе, указан ряд конкретных деталей. Однако следует понимать, что варианты реализации настоящего изобретения могут быть реализованы на практике без этих конкретных деталей. В других случаях хорошо известные способы, структуры и технологии не были показаны в деталях, чтобы не затруднять понимание данного описания.

Терминология.

При описании предпочтительного варианта реализации настоящего изобретения, изображенного на чертежах, из соображений ясности была использована конкретная терминология. Однако настоящее изобретение не должно ограничиваться конкретными терминами, выбранными таким образом, и следует понимать, что каждый конкретный термин включает все технические эквиваленты, которые работают подобным образом для достижения подобной технической цели. Термины, такие как "передний", "задний", "радиально", "периферически", "вверх", "вниз" и подобные, используются как слова для удобства, чтобы обозначить точки отсчета, и не должны рассматриваться как ограничивающие термины.

Содержащий и включающий.

В формуле изобретения, которая следует далее, и в предыдущем описании настоящего изобретения, за исключением случаев, где контекст требует другого ввиду определенного выражения или необходимого значения, слово "содержать" или такие варианты как "содержит" или "содержащий" используются во включающем смысле, т.е. для определения наличия приведенных признаков, но не исключая наличие или добавление дополнительных признаков в различных вариантах реализации настоящего изобретения.

Любой из терминов: включая, или что включает, или который включает, -при использовании в данном документе также является открытым выражением, что также означает включение, по меньшей мере, элементов/признаков, которые следуют за термином, но не исключают другие. Таким образом, "включающий" является синонимом и означает "содержащий".

Объем настоящего изобретения.

Таким образом, несмотря на то, что было описано то, что считается предпочтительными вариантами реализации настоящего изобретения, специалистам в данной области техники будет ясно, что другие и дополнительные модификации можно сделать в нем без отклонения от сущности изобретения, и предполагается, что все такие изменения и модификации попадают в объем настоящего изобретения. Например, любые формулы, данные выше, являются только иллюстративными для процедур, которые могут быть использованы. Функции могут быть добавлены или удалены из блок-схем, а операции могут быть взаимно заменены в функциональных блоках. Этапы могут быть добавлены или удалены из способов, описанных в объеме настоящего изобретения. Несмотря на то, что настоящее изобретение было описано со ссылкой на конкретные примеры, специалистам в данной области техники будет ясно, что настоящее изобретение может быть реализовано во многих других формах.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ проверки подлинности информации документа, включающий

этап создания записи о проверке, включающий

прием метаданных содержимого документа из документа;

генерирование хеша метаданных, используя метаданные содержимого документа;

создание блокчейн-транзакции, используя хеш метаданных;

генерирование читаемых компьютером данных, кодирующих хеш метаданных; и

обновление документа читаемыми компьютером данными; и

этап обновления содержимого документа, включающий

прием обновленных метаданных содержимого документа для документа;

генерирование дополнительного хеша метаданных, используя обновленные метаданные содержимого документа;

создание дополнительной блокчейн-транзакции, используя дополнительный хеш метаданных;

этап проверки документа, включающий

прием документа;

извлечение хеша метаданных из читаемых компьютером данных;

идентификацию блокчейн-транзакции блокчейна для проверки подлинности метаданных документа; и дополнительно включающий

проверку блокчейна в обратном хронологическом порядке для идентификации дополнительной блокчейн-транзакции для определения, что метаданные содержимого документа заменены обновленными метаданными содержимого документа.

2. Способ по п.1, в котором создание блокчейн-транзакции, используя хеш метаданных, включает сохранение идентификатора документа и хеша метаданных в блокчейне, а создание дополнительной блокчейн-транзакции включает сохранение идентификатора документа и дополнительного хеша метаданных в блокчейне; и при этом проверка блокчейна в обратном хронологическом порядке включает поиск в блокчейне с использованием идентификатора документа.

3. Способ по п.1, в котором читаемые компьютером данные представляют собой штрих-код.

4. Способ по п.3, в котором штрих-код представляет собой двухмерный штрих-код.

5. Способ по п.1, в котором этап создания записи о проверке дополнительно включает подписание документа закрытым ключом, связанным с сервером проверки документа.

6. Способ по п.1, дополнительно включающий сохранение метаданных содержимого документа, так что при этом этап проверки документа дополнительно включает извлечение метаданных содержимого документа и отображение метаданных содержимого документа.

7. Способ по п.6, в котором сохранение метаданных содержимого документа включает кодирование метаданных содержимого документа в читаемых компьютером данных.

8. Способ по п.6, в котором сохранение метаданных содержимого документа включает кодирование метаданных содержимого документа в блокчейн-транзакции.

9. Способ по п.1, в котором этап создания записи о проверке дополнительно включает идентификацию метаданных содержимого документа из документа.

10. Способ по п.9, в котором идентификация метаданных содержимого документа включает оптическое распознавание символов.

11. Способ по п.10, в котором идентификация метаданных содержимого документа включает выполнение запросов строки для поиска в тексте, извлеченном при помощи оптического распознавания символов.

12. Способ по п.10, в котором идентификация метаданных содержимого документа включает выделение текста по меньшей мере в одной определенной пользователем области документа.

13. Способ по п.1, дополнительно включающий идентификацию того, какой из документов заменен.

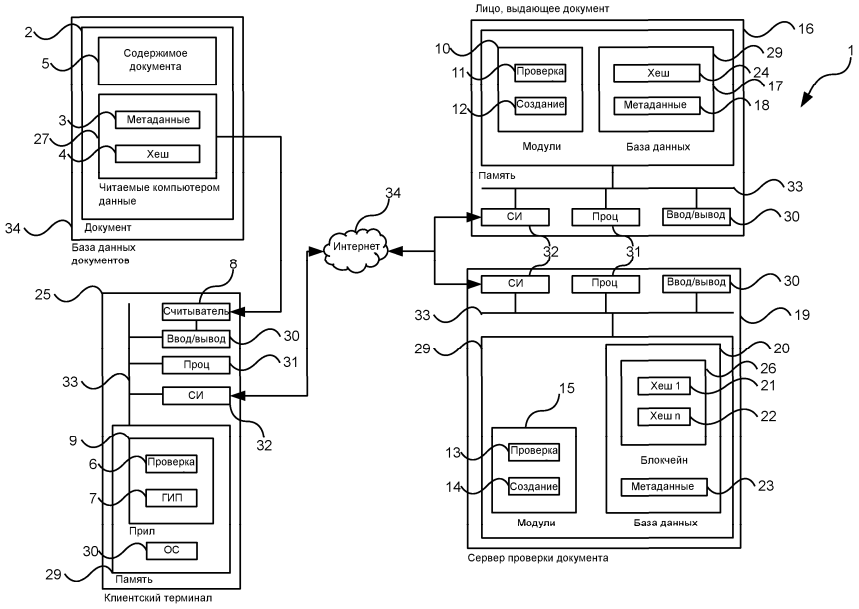
14. Способ по п.1, дополнительно включающий этап аннулирования проверки документа, включающий

создание блокчейн-транзакции аннулирования, так что на этапе проверки документа способ дополнительно включает

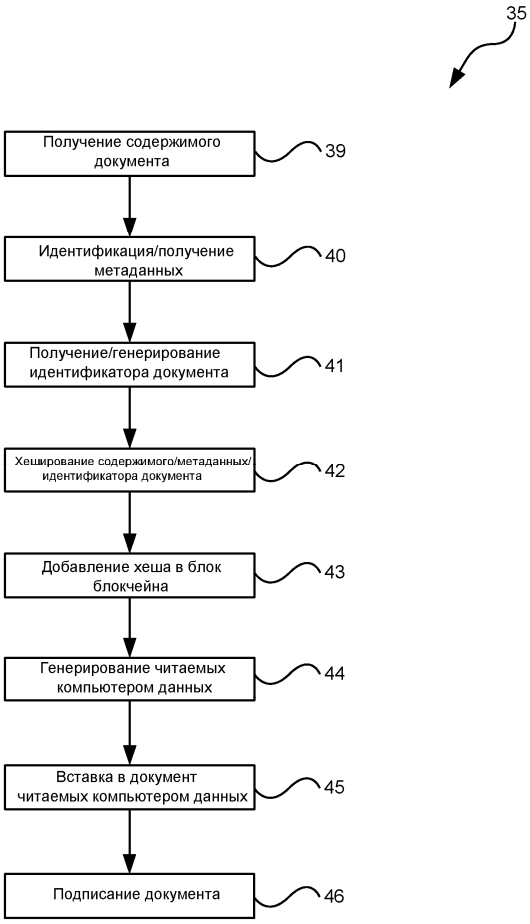
идентификацию блокчейн-транзакции аннулирования, следующей по времени за блокчейн-транзакцией, для завершения неудачей проверки подлинности информации документа.

15. Способ по п.1, в котором блокчейн-транзакция также определяет срок валидности, так что на этапе проверки документа способ дополнительно включает завершение неудачей проверки документа, если срок валидности истек.

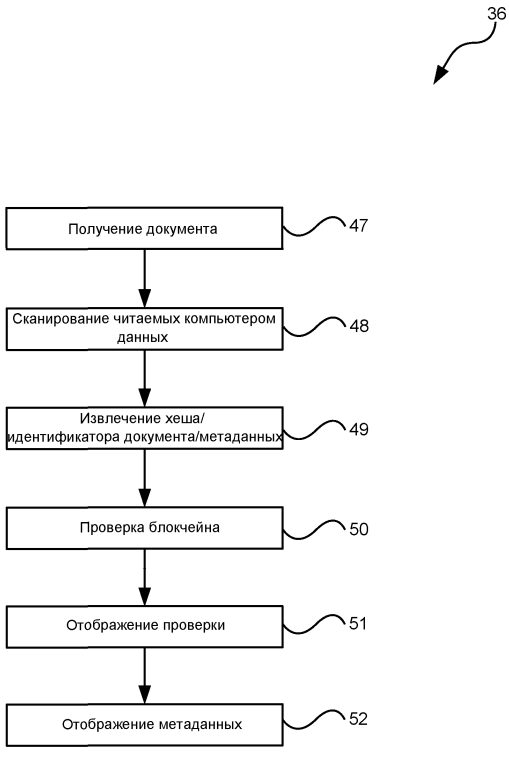
16. Способ по п.15, дополнительно включающий создание блокчейн-транзакции восстановления срока валидности, содержащей дополнительный срок валидности, так что на этапе проверки документа дополнительный срок валидности используют при определении валидности документа.



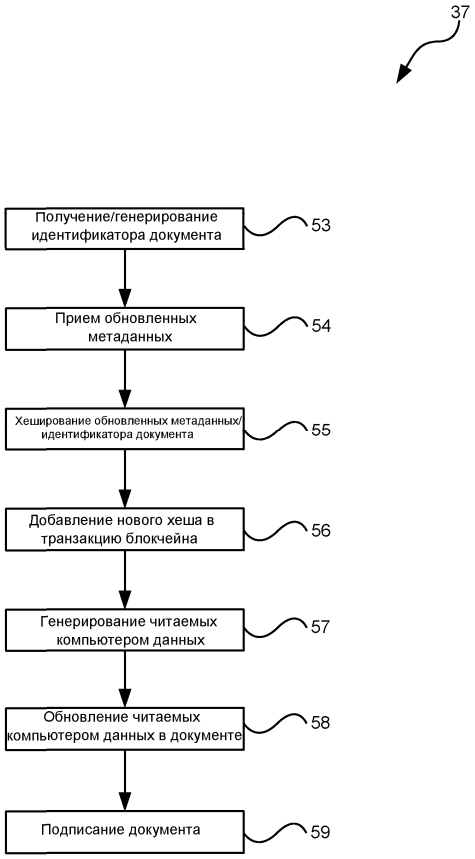
Фиг. 1


35
Получение содержимого документа
39
Идентификация/получение метаданных
40
Получение/генерирование идентификатора документа
41
Хеширование содержимого/метаданных/ идентификатора документа
42
Добавление хеша в блок блокчейна
43
Генерирование читаемых компьютером данных
44
Вставка в документ читаемых компьютером данных
45
Подписание документа
46

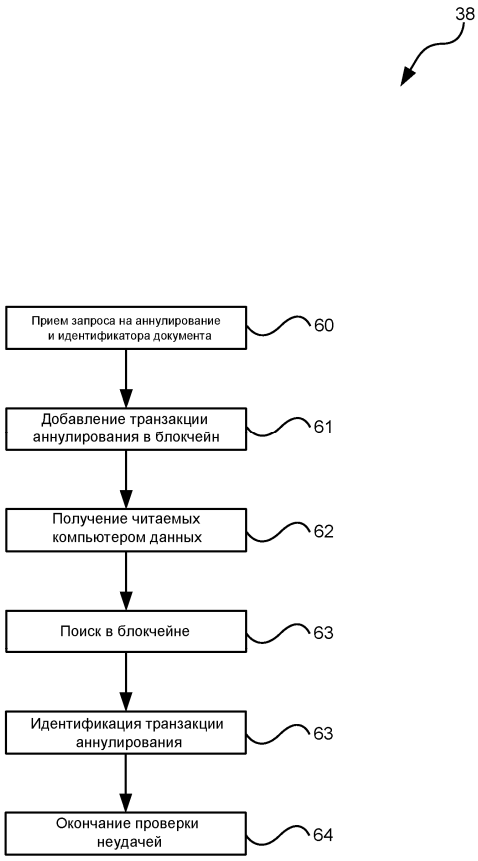
Фиг. 2


36
Получение документа
47
Сканирование читаемых компьютером данных
48
Извлечение хеша/ идентификатора документа/метаданных
49
Проверка блокчейна
50
Отображение проверки
51
Отображение метаданных
52

Фиг. 3


37
Получение/генерирование идентификатора документа
53
Прием обновленных метаданных
54
Хеширование обновленных метаданных/ идентификатора документа
55
Добавление нового хеша в транзакцию блокчейна
56
Генерирование читаемых компьютером данных
57
Обновление читаемых компьютером данных в документе
58
Подписание документа
59

Фиг. 4


38
Прием запроса на аннулирование и идентификатора документа
60
Добавление транзакции аннулирования в блокчейн
61
Получение читаемых компьютером данных
62
Поиск в блокчейне
63
Идентификация транзакции аннулирования
63
Окончание проверки неудачей
64

Фиг. 5


28
Документ
Сертификат о присвоении квалификации
Сертификат о присвоении квалификации выдается зарегистрированной обучающей организацией, когда лицо окончило один или более аккредитованных модулей
ALWEST
TRAINING SERVICE
РОББАР ПТИ ЛТД
Национальный код поставщика услуг № 51925
Данный сертификат подтверждает, что
Джеймс Смит
получил квалификацию
RIIMPO311A
Эксплуатация карьерных самосвалов
Боб Купер
Руководитель
дата 7 июля 2007
документ 0007/07/2007

Фиг. 6