РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 722 285**(13) **C1**

(51) МПК
G06K 5/02 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06K 5/02 (2020.02); G06Q 10/08 (2020.02); G06Q 30/00 (2020.02)

(21)(22) Заявка: **2019144325, 27.12.2019**

(24) Дата начала отсчета срока действия патента:
27.12.2019

Дата регистрации:
28.05.2020

Приоритет(ы):
(22) Дата подачи заявки: **27.12.2019**

(45) Опубликовано: **28.05.2020** Бюл. № **16**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Шишкин Евгений Сергеевич (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2709288 C1, 17.12.2019. RU 2679545 C1, 11.02.2019. RU 2643503 C1, 01.02.2018. RU 2639015 C1, 19.12.2017. US 2018/0094953 A1, 05.04.2018.**

(54) Способ проверки подлинности изделий

(57) Реферат:

Изобретение относится к проверке подлинности изделий. Технический результат заключается в расширении арсенала средств. Способ реализуется с использованием системы, содержащей базу данных (БД) типа публичный блокчейн, связанную с сетью Интернет и выполненную с возможностью назначать идентификаторы пользователям БД, осуществлять вызовы запрограммированных пользователями функций по управлению данными (смарт-контракт), которые способны выполнять следующие действия: в случае если изделие с заданным идентификатором отсутствует в БД, добавлять идентификатор изделия и указывать соответствие этого идентификатора изделия идентификатору производителя, менять соответствие между идентификатором изделия и идентификатором владельца при наличии электронной цифровой подписи (ЭЦП) от текущего владельца изделия и ЭЦП нового владельца; менять соответствие между идентификатором изделия и идентификатором владельца при указании цепочки транзакций между владельцами с указанием корректных ЭЦП всех промежуточных владельцев, добавлять смарт-контракты пользователей; причем при очередной передаче изделия текущий владелец посылает подписанную своей подписью транзакцию напрямую следующему владельцу, избегая необходимости производить транзакцию в блокчейн, обеспечивая анонимность покупателю. 1 з.п. ф-лы.

RU 2722285 C1

RU 2722285 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 722 285**(13) **C1**

(51) Int. Cl.
G06K 5/02 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06K 5/02 (2020.02); *G06Q 10/08* (2020.02); *G06Q 30/00* (2020.02)

(21)(22) Application: **2019144325, 27.12.2019**

(24) Effective date for property rights:
27.12.2019

Registration date:
28.05.2020

Priority:
(22) Date of filing: **27.12.2019**

(45) Date of publication: **28.05.2020** Bull. № **16**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Shishkin Evgenij Sergeevich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2722285 C1

(54) AUTHENTICATION METHOD OF ARTICLES

(57) Abstract:

FIELD: authentication of articles.

SUBSTANCE: method is realized using a system comprising a database (DB) such as a public blockchain connected to the Internet and configured to assign identifiers to DB users, perform calls to user-programmed data management functions (smart contract), which are capable of performing the following actions: in case the article with the specified identifier is absent in the DB, add product identifier and indicate compliance of this product identifier with manufacturer identifier, to change conformity between product identifier and owner identifier in presence of electronic digital signature (EDS) from current owner of product and EDS of new owner; to change conformity between product identifier and owner identifier when specifying chain of transactions between owners with indication of correct EDS of all intermediate owners, to add smart contracts of users; wherein during the next transfer of the product, the current owner sends the transaction signed by his / her signature directly to the next owner, avoiding the need to perform transaction in the blockchain, providing anonymity to the buyer.

EFFECT: technical result is wider range of means.

1 cl

RU 2722285 C1

Область техники, к которой относится изобретение

Предполагаемое изобретение относится к методам отслеживания подлинности изделия, контроля и уменьшения вероятности появления контрафактных копий.

Уровень техники

В настоящее время известны различные способы проверки подлинности изделий.

Среди перспективных можно отметить способы с использованием записи информации об изделии и текущем владельце в базу данных (БД) типа публичный блокчейн. Далее в тексте под БД будет подразумеваться именно БД типа публичный блокчейн

Помимо идентификатора самого изделия, в БД записывается идентификатор каждого последующего владельца изделия, образуя непрерывную цепочку. При очередной передаче, участник, желающий принять изделие во владение, может проверить, что изделие, находящееся перед ним, действительно подлинное, путем сравнения информации о текущем владельце по уникальному идентификатору изделия в БД, а также удостовериться, что изделие с данным идентификатором в самом деле было произведено.

Идентификатор каждого владельца, записанного за изделием, связан с открытым ключом ключевой пары, с помощью которой формируется ЭЦП транзакции в БД, таким образом наличие ключевой пары у человека подтверждает аутентичность всех операций, проведенных в БД.

Известен способ проверки подлинности изделий (патент РФ №2679545, приоритет от 24.04.2018) с использованием технологии блокчейн и технологии смарт-контрактов на ее основе. Применение известного способа обеспечивает возможность сохранения всей истории владения, при этом существенно сокращая количество проводимых транзакций в БД, за счет этого достигается более высокая скорость обработки и снижение стоимости эксплуатации системы.

При использовании технологии блокчейн, тем не менее, у ряда пользователей, в силу различных обстоятельств и желаний, возникает потребность сохранения анонимности при совершении сделок.

Однако, известный способ не позволяет обеспечить анонимность при совершении сделок, что является его недостатком.

Известен также способ с использованием БД типа блокчейн (Погружение в технологию блокчейн: борьба с контрафактными товарами - статья по адресу https://habrahabr.ru/company/microsoft/blog/312054/), согласно которому

- при производстве очередного изделия, назначают уникальный идентификатор;
- наносят назначенный идентификатор на изделие;
- ставят в соответствие идентификатору произведенного изделия публично известный идентификатор производителя изделий, и записывают данное соответствие в БД блокчейн;
- (А) при передаче изделия следующему владельцу, передающая сторона посылает в блокчейн транзакцию о передаче прав на изделие следующему владельцу, указывая при этом идентификатор нового владельца;
- посылают транзакцию в блокчейн от принимающей стороны о согласии на принятие изделия во владение; ставят в соответствие идентификатору изделия идентификатор нового владельца и записывают данное соответствие в базу данных блокчейн;
- при последующих передачах переходят к пункту А.

Данный способ принят за прототип.

Тем не менее, известный способ также имеет недостаток - отсутствие возможности для покупателя остаться анонимным.

Раскрытие сущности изобретения

Техническим результатом является обеспечение возможности для владельцев изделий, при их желании, остаться анонимными.

Для этого предлагается способ проверки подлинности изделий, реализуемый с использованием системы, содержащей

- базу данных (БД) типа публичный блокчейн, связанную с сетью Интернет и выполненную с возможностью
  - назначать идентификаторы пользователям БД;
  - осуществлять вызовы запрограммированных пользователями функций по управлению данными (смарт-контракт), которые способны выполнять следующие действия:
    - производить вычисление выбранной владельцем смарт-контракта функции A(x), где x - натуральное число;
    - в случае, если изделие с заданным идентификатором отсутствует в БД, добавлять идентификатор изделия и указывать соответствие этого идентификатора изделия идентификатору производителя;
    - получать идентификатор владельца по заданному идентификатору изделия;
    - получать значение слепка пароля по заданному идентификатору изделия
    - посылать запрос на изменение соответствия идентификатора изделия идентификатору текущего владельца на идентификатор нового владельца при наличии электронной цифровой подписи (ЭЦП) текущего владельца;
    - подтверждать изменение соответствия между идентификатором изделия и идентификатором владельца на соответствие идентификатору нового владельца при наличии ЭЦП нового владельца;
    - отменять изменение соответствия идентификатора изделия идентификатору текущего владельца на идентификатор нового владельца при наличии ЭЦП текущего владельца;
    - изменять соответствие между идентификатором изделия и значением маски пароля с одновременным обнулением значения идентификатора текущего владельца изделия при наличии ЭЦП текущего владельца;
    - изменять соответствие между идентификатором изделия и производным значением пароля на новое производное значение пароля при предъявлении искомого действующего пароля
    - изменять соответствие между идентификатором изделия и идентификатором владельца при наличии пароля r, значение от которого A(r) соответствует сохраненному ранее производному значению пароля
  - добавлять смарт-контракты пользователей;
- средство формирования доказательства вычисления без разглашения (далее СФДВ), выполненное с возможностью:
  - формировать ключ построения доказательства pk и ключ проверки доказательства vk с использованием функции A(x) в качестве параметра;
  - формировать блок данных доказательства Prf и численное значение b с использованием функции A(x) в качестве параметра, ключа формирования доказательств pk и численного значения d, причем A(d)=b
  - верифицировать блок данных доказательства Prf с использованием функции A (x) в качестве параметра, ключа проверки доказательств vk и значения b,
  - получать и передавать данные; способ заключается в том, что
- выбирают функцию A(x), такую, что вычислительно трудно определить значение

b по заданному значению c, причем A(b)=c;

- формируют ЭЦП производителя;
- назначают в БД уникальный идентификатор производителя;
- формируют в СФД B ключ проверки доказательства vk и ключ построения доказательств pk с использованием функции A(x);
- формируют смарт-контракт в БД, содержащий функцию A(x), идентификатор производителя, значения ключа построения доказательств pk и ключа проверки доказательств vk;
- если произведено новое изделие, то
  - назначают уникальный идентификатор изделию;
  - наносят назначенный идентификатор на изделие;
  - записывают в БД через смарт-контракт данные о соответствии идентификатора изделия идентификатору производителя; при необходимости передать изделие от производителя покупателю,
- формируют ЭЦП покупателя;
- в случае, если покупатель желает закрепить свой статус владения в БД выполняют следующие действия:
  - если у покупателя отсутствует идентификатор в БД, назначают в БД уникальный идентификатор покупателю;
  - на стороне производителя, через смарт-контракт, посылают запрос на изменение соответствия идентификатора передаваемого изделия идентификатору покупателя, подписывая запрос ЭЦП производителя;
  - на стороне покупателя, через смарт-контракт, подтверждают изменение соответствия между идентификатором передаваемого изделия и идентификатором покупателя, подписывая запрос ЭЦП покупателя;
  - производят передачу изделия от производителя покупателю;
- в случае, если покупатель желает остаться анонимным, выполняют следующие действия:
  - на стороне покупателя, производят проверку соответствия идентификатора изделия идентификатору производителя через БД
  - на стороне покупателя, генерируют пароль r и вычисляют производное значение пароля h=A(r);
  - на стороне покупателя, сохраняют пароль r;
  - передают значение h от покупателя производителю;
  - на стороне покупателя, выполняют условие завершения сделки;
  - на стороне производителя, через смарт-контракт, изменяют соответствие идентификатора изделия производному значению пароля h, подписывая транзакцию ЭЦП производителя;
  - на стороне покупателя, через смарт-контракт, получают текущее значение производного значения пароля hp для передаваемого изделия
  - если значение hp не равно h, то прерывают сделку;
  - производят передачу изделия от производителя покупателю; при необходимости передать изделие от продавца покупателю,
- формируют ЭЦП покупателя;
- формируют ЭЦП продавца;
- в случае, если соответствие идентификатора передаваемого изделия

идентификатору продавца зафиксировано в БД, и покупатель желает также закрепить свой статус владения в БД, то выполняют следующие действия:

- если у покупателя отсутствует идентификатор в БД, назначают уникальный идентификатор покупателю в БД;
- на стороне продавца, через смарт-контракт, формируют запрос на изменение соответствия идентификатора передаваемого изделия идентификатору покупателя, подписывая запрос ЭЦП продавца;
- на стороне покупателя, через смарт-контракт, подтверждают изменение соответствия идентификатора изделия идентификатору покупателя, подписывая транзакцию ЭЦП покупателя;
- производят передачу изделия от продавца покупателю;

- в случае, если соответствие идентификатора передаваемого изделия идентификатору продавца зафиксировано в БД, а покупатель желает остаться анонимным, то выполняют следующие действия:

- проверяют подлинность изделия путем сравнения идентификатора текущего владельца передаваемого изделия, записанного в БД и идентификатора продавца;
- если идентификаторы не совпали, то прерывают сделку;
- на стороне покупателя, генерируют пароль r1 и вычисляют производное значение пароля h1=A(r1);
- сохраняют пароль r1 на стороне покупателя;
- передают значение h1 от покупателя продавцу;
- на стороне покупателя, выполняют условие завершения сделки;
- на стороне продавца, в смарт-контракте, меняют соответствие между идентификатором изделия и производным значением пароля на новое значение h1, подписывая транзакцию с помощью ЭЦП продавца;
- на стороне покупателя, через смарт-контракт, получают текущее производное значение пароля h2, соответствующее идентификатору передаваемого изделия;
- если значение h2 не равно h1, то прерывают сделку;
- производят передачу изделия от продавца покупателю;

- в случае, если соответствие идентификатора передаваемого изделия идентификатору продавца не зафиксировано в БД, и покупатель желает остаться анонимным, то выполняют следующие действия:

- на стороне продавца, запрашивают из смарт-контракта ключ построением доказательств pk;
- на стороне продавца, используя СФДВ, формируют блок доказательства prf2 с использованием функции A(x), пароля r, сохраненного на стороне продавца, и ключа построения доказательств pk;
- передают блок доказательства prf2 от продавца покупателю;
- на стороне покупателя, запрашивают из БД ключ проверки доказательств vk;
- на стороне покупателя, через смарт-контракт, получают производное значение пароля h, соответствующее передаваемому изделию;
- на стороне покупателя, используя СФДВ, производят проверку блока доказательства prf2 с использованием функции A(x), производного значения пароля h и ключа vk;
- если проверка неуспешна, то прерывают сделку;

- на стороне покупателя, формируют пароль r2;
- на стороне покупателя, вычисляют производное значение пароля h2=A(r2);
- на стороне покупателя, сохраняют пароль r2;
- отправляют значение h2 от покупателя продавцу;
- на стороне покупателя, выполняют условие завершения сделки;
- на стороне продавца, отправляют производителю запрос на изменение соответствия идентификатора изделия новому производному значению пароля h2, передавая текущий пароль r;
- на стороне производителя, через смарт-контракт меняют соответствие между идентификатором передаваемого изделия и производным значением пароля на новое значение h2, предъявляя текущий пароль r и подписывая транзакцию ЭЦП производителя;
- если покупатель устанавливает, что производное значение пароля для передаваемого изделия не изменилось в БД, или изменилось, но не равно h2, то прерывают сделку;
- производят передачу изделия от продавца покупателю;
- в случае, если соответствие идентификатора передаваемого изделия идентификатору продавца не зафиксировано в БД, а покупатель желает закрепить свой статус владения в БД, то выполняют следующие действия:
- если у покупателя отсутствует идентификатор в БД, назначают уникальный идентификатор покупателю;
- если у покупателя отсутствует ЭЦП, формируют ЭЦП покупателя;
- на стороне продавца, в смарт-контракте, запрашивают ключ построения доказательства pk,
- на стороне продавца, используя СФДВ, формируют блок данных доказательства prf3, используя в качества параметров функцию A(x), ключ построения доказательств pk и пароля r3;
- производят передачу блока доказательства prf3 от продавца покупателю;
- на стороне покупателя, в смарт-контракте, запрашивают ключ проверки доказательства vk;
- на стороне покупателя, в смарт-контракте, запрашивают производное значение от пароля h3, соответствующую передаваемому изделию;
- на стороне покупателя, используя СФДВ, производят проверку блока доказательства, используя в качестве параметров функцию A(x), ключ проверки доказательств vk, производное значение от пароля h3 и блок данных доказательства prf3;
- если проверка неуспешна, то прерывают сделку;
- на стороне покупателя, выполняют условие завершения сделки;
- передают пароль r3 от продавца покупателю;
- на стороне покупателя, через смарт-контракт, меняют соответствие идентификатора изделия идентификатору покупателя, используя переданный пароль r3;
- передают изделие от продавца покупателю.

В качестве функции A(x) может быть выбрана криптографическая хэш-функция.

Способ в своей основе опирается на ряд предположений о мотивации и поведении участников системы:

- у каждого изделия и владельца имеется уникальный идентификатор;
- изделие нельзя передать сразу нескольким владельцам;
- участник - владелец изделия - должен иметь возможность доказать другому участнику, что изделие с данным идентификатором действительно принадлежит именно ему;
- статус владения изделием должен меняться только в случае фактической передачи изделия от одного участника к другому, с обоюдного согласия каждой стороны;
- должна быть возможность скрыть факт владения изделием, но при этом сохранена возможность дальнейшей передачи изделия, с возможностью установить факт аутентичности изделия.

Для обеспечения работы предлагаемого способа должно быть предварительно создано и введено в действие средство формирования доказательства вычисления без разглашения (СФДВ).

Средство СФДВ может быть выполнено в программном, программно-аппаратном или полностью аппаратном виде, но предпочтительным является вариант программного исполнения в виде ПО, которое устанавливается на вычислительное устройство производителя изделий и покупателей.

Предполагается, что у производителя изделий есть мотивация к корректной надежной работе такой системы (борьба с контрафактом снижает потенциальные убытки).

Очередной участник - владелец изделия - может быть заинтересован в публикации факта владения в открытом источнике, но может и предпочитать оставаться анонимным: система должна позволять реализовывать оба сценария.

При передаче изделия от текущего владельца к следующему, участники ведут себя рационально, т.е. делают все, чтобы с минимальными издержками прийти к желаемой цели.

Идентификатор владельца не меняется со временем. У владельца имеется только один, закрепленный именно за ним, идентификатор.

Из-за требования о неизменяемости данных, централизованные решения, основанные на классических базах данных, здесь не подходят. Нецелесообразно передавать все полномочия по управлению данными и бизнес-логикой в руки одной стороны либо даже консорциума, поэтому в качестве платформы выбрана БД типа публичный блокчейн: БД этого типа дает гарантии на неизменность и высокую доступность сохраняемой информации без необходимости доверять управление третьим лицам.

Для того, чтобы обеспечить всем участникам процесса одинаковую осведомленность об изменениях данных в системе, а также гарантировать, что правила, по которым данные преобразуются, не могут поменяться, бизнес-логика управления цепочкой владения оформляется в виде смарт-контракта с доступным для всех открытым кодом.

Чтобы система была устойчивой к возможным DDoS-атакам, ее размещают на блокчейн-платформе с большим количеством участвующий вычислительных узлов.

Подобное решение было предложено, например, в способе-прототипе. Решение покрывает большую часть заявленных требований, но есть и недостатки.

Недостатком способа-прототипа при этом можно также считать отсутствие возможности сокрытия какой-то части цепочки владения: например, бывает так, что логистика является одной из составных частей конкурентного преимущества бизнеса, и публикация идентификаторов контрагентов может выдать эту информацию заинтересованным лицам. Или же человек, принимающий во владение какую-то вещь, не желает по каким-либо своим причинам фиксировать факт владения в общественно

доступной БД.

Если участник, принимающий изделие во владение, будет посылать транзакцию в блокчейн, это неизбежно приведет к публикации его идентификатора (на данный момент, большинство блокчейн-платформ не поддерживают анонимные транзакции).

Для решения проблемы приватных передач изделий между владельцами в предлагаемом способе используется криптографический протокол неинтерактивного доказательства с нулевым разглашением, реализованный в средстве СФДВ.

Доказательство с нулевым разглашением - это совокупное название способов, позволяющих доказать факт обладания решением какой-то вычислительной задачи другой стороне, без необходимости предъявлять решение проверяющей стороне. Например, такой задачей может быть поиск прообраза хэш-функции по заданному образу.

Изначальное развертывание системы выполняет производитель изделий, выполняя следующие действия.

1. Производитель изделий выбирает всюду определенную функцию A(x), такую, чтобы отыскать прообраз по заданному образу было вычислительно трудно. Например, положим A(x) = SHA256(x), где SHA256(x) - криптографическая хэш-функция. Здесь и далее, мы будем называть пару значений r и h, таких, что A(r) = h, следующими терминами: значение r - паролем, значение h - производным значением от пароля r.

2. Производитель изделий, используя средство СФДВ, генерирует ключ построения доказательств pk и ключ проверки доказательств vk для функции A(x).

3. Производитель публикует ключи pk и vk в открытом общедоступном источнике, таком как веб-сайт или публичной БД типа блокчейн.

4. Производитель изделий создает смарт-контракт в БД.

Смарт-контракт содержит следующие функции:

- функцию, вычисляющая выбранную функцию A(x); в рассматриваемом примере эта функция совпадает с функцией SHA256(x);
- addItem (itemId): добавляет изделие с идентификатором itemId в БД; в качестве владельца назначается идентификатор производителя изделий;
- requestChangeHolder (itemId, newHolder): начинает процедуру передачи прав на изделие itemId от текущего владельца владельцу с идентификатором newHolder; для завершения процедуры передачи требуется, чтобы участник с идентификатором newHolder вызвал функцию ackChangeHolder, таким образом, подтвердив свое желание получить изделие во владение;
- ackChangeHolder (itemId): подтвердить намерение оформления изделия itemId во владение;
- cancelChangeHolder (itemId): отменить ранее инициированную процедуру передачи изделия;
- getItemHolder (itemId): возвращает идентификатор владельца изделия с номером itemId;
- anonymizeItem (itemId, H): поставить значение текущего владельца для изделия с номером itemId в значение undefined (т.е. не определено), установив при этом производное значение пароля для данного изделия равным H;
- changeHashKey (itemId, R, H): установить новое производное значение от пароля H для изделия itemId, предварительно предъявив пароль R, производное значение от которого равно текущему производному значению пароля для данного изделия;
- changeHolderByKey (itemId, R, newHolder): для изделия с идентификатором itemId, в случае, если текущий владелец изделия не выставлен (т.е. значение undefined), и, если

производное значение переданного пароля R равно текущему производному значению пароля для изделия itemId, установить идентификатор текущего владельца равным newHolder.

5. Добавлять идентификаторы изделий по мере необходимости

Все произведенные изделия изначально числятся за производителем, чей идентификатор заранее известен.

Известной реализацией средства СФДВ можно считать алгоритмы семейства zkSNARK. Рассмотрим принцип их работы с прикладной точки зрения. Описание внутреннего устройства алгоритмов раскрывается (Описание криптографического протокола zkSNARK - статья по адресу https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof).

Пусть имеется вычислительная задача, заданная функцией C(x). Функция C(x) известна обоим участникам протокола. Допустим, участник A желает доказать участнику B факт того, что знает такое значение w, что C(w) удовлетворяет какому-либо критерию, например, C(w) = *a*, но при этом не желает предъявлять само значение w в открытом виде, а значение *a* известно обоим участникам.

Метод zkSNARK состоит из следующих шагов.

1. Доверенная 3-я сторона запускает функцию-генератор POC_GEN для заданной функции C(x), получая на выходе пару значений: pk - ключ доказательства, vk - ключ проверки:

POC_GEN(C(x))=(pk, vk)

Значения pk и vk могут быть опубликованы в общедоступном месте, например, на веб-сайте компании-производителя. Можно обратить внимание на тот факт, что функция-генератор POC_GEN на вход принимает некоторую всюду определенную вычислимую функцию. Способ описания функции может быть различным, в зависимости от реализации метода, например, в виде арифметических схем.

2. Участник A выполняет построение блока данных доказательства prf, выполняя функцию построения блока доказательства POC_PROOF:

POC_PROOF (C(x), pk, *a*, w) = prf

Блок данных доказательства prf передается стороне B.

3. Участник B проверяет блок данных доказательства prf выполняя функцию проверки блока доказательства POC_VERIFY.

Если

POC_VERIFY (C(x), vk, *a*, prf) = Истина,

то доказательство считается состоятельным, и участник A действительно обладает значением w, таким что C(w) = *a*.

Специализированные функции POC_GEN, POC_PROOF, POC_VERIFY образуют ядро метода zkSNARK.

Параметры pk и vk для функции C(x) генерируются доверенной 3-й стороной в виде переменных смарт-контракта и не меняются со временем. В нашем случае это делает производитель изделий, при размещении смарт-контракта в БД.

Рассмотрим возможные сценарии передачи изделия от одного участника к следующему участнику. Под участником понимается владелец изделия, покупатель изделия или производитель изделий. Здесь, в качестве функции C(x) используется SHA256 (x).

Сценарий 1. Передача изделия от публичного участника A другому участнику B, желающему остаться анонимным.

1. Участник B проверяет подлинность изделия путем проверки соответствия

идентификатора изделия идентификатору участника A, который тот предъявляет B, например, путем формирования электронной цифровой подписи (ЭЦП) для блока данных, содержащего идентификатор изделия, и посылки подписанного блока данных от A к B. Участник B извлекается из подписанного блока данных публичный ключ подписавшей стороны.

В качестве алгоритма ЭЦП может использоваться, например, алгоритм ECDSA с эллиптической кривой secp256k1 (Стандарт NIST на протокол ECDSA - статья по адресу https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf). Данный алгоритм позволяет узнать публичный ключ подписавшей стороны, если известна подписываемая информация.

В случае, если в качестве БД используется система Ethereum, то идентификатор пользователя - владельца публичного ключа вычисляется как

Userld=SHA256 (PubKey)

2. Участник B генерирует пароль R_B и вычисляет производное значение пароля H_B=SHA256(R_B), сохраняя R_B в надежном месте.

3. Участник B передает предоплату стороне A за изделие.

4. Участник B передает стороне A значение H_B с требованием поменять производное значение пароля для изделия в БД путем выполнения транзакции anonymizeltem (itemId, H_B), при этом публичный адрес текущего владельца изделия выставляется как undefined. Транзакция проводится от участника A, поэтому подписывается ЭЦП участника A.

5. Участник B убеждается в изменении производного значения для изделия в БД, после чего участники A и B обмениваются ценностями: остаток оплаты меняется на изделие.

Сценарий 2: Передача изделия между анонимным участником B и участником C, желающим также остаться анонимным. Роль доверенного лица играет третий участник - например, производитель изделий.

1. Участник B, используя средство СФДВ и известный ключ построения доказательств, генерирует блок данных доказательства обладания паролем R_c для передаваемого изделия.

2. Участник B передает блок данных доказательства участнику C.

3. Участник C, используя средство СФД B и известный ключ проверки доказательств, проводить проверку переданного блока данных доказательства.

4. Участник C формирует пароль R_C такой, что H_C=SHA256 (R_C).

5. Участник C вносит предоплату за изделие.

6. Участник C отправляет участнику B значение H_C, сохраняя R_C в надежном месте.

7. Участник B обращается к производителю изделий с запросом о замене производного значения пароля изделия H_C, используя как доказательство владения пароль R_B (участник B обладает паролем согласно сценарию 1).

8. Производитель вызывает транзакцию changeHashKey (itemId, Rb, H_C), изменяя устанавливая соответствие изделию нового производного значения пароля H_C, предъявляя для этого пароль R_b.

9. Участники C и B обмениваются ценностями: участник B получает оставшуюся часть оплаты, а участник C получает изделие.

Заметим, что ни участник B, ни участник C не производят транзакций в смарт-контракте, но при этом на каждом этапе у участников есть возможность предъявить и проверить доказательство владения изделием. Закрепить право на изделие без

необходимости прямого вызова в БД возможно благодаря наличию надежного посредника в лице участника A, который проводит транзакцию от своего имени. Таким участником может выступать, например, производитель изделия.

Сценарий 3: Передача изделия происходит между анонимным участником C и участником D, желающим записать свой статус владельца в БД.

1. Участник B, используя средство СФДВ и известный ключ построения доказательств, генерирует блок данных доказательства обладания паролем R_c для передаваемого изделия.

2. Участник B передает блок данных доказательства участнику C.

3. Участник C, используя средство СФДВ и известный ключ проверки доказательств, проводить проверку переданного блока данных доказательства.

4. Участник D вносит предоплату за изделие.

5. Участник C передает D пароль R_C.

6. Участник D выполняет транзакцию changeHolderByKey (itemId, R_C, D), предъявляя текущий пароль R_C и устанавливая в результате идентификатор текущего владельца изделия itemId равным D.

7. Участники завершают сделку, производя обмен изделия на оставшуюся часть оплаты.

Сценарий 4: Передача изделия происходит между публичным владельцем A и участником B, желающим также закрепить свой статус в БД.

1. Участник B вносит предоплату.

2. Участник A вызывает requestChangeHolder (itemId, B), тем самым запрашивая у участника B разрешение на передачу статуса владения изделием itemId.

3. Участник B вызывает ackChangeHolder (itemId), подтверждая согласие на обладание изделием.

4. Участники завершают сделку, производя обмен изделия на оставшуюся часть оплаты.

Далее предлагаемый способ проанализирован с точки зрения возможного поведения участников в рамках заданного представления об их мотивах. Анализируются только те шаги, где происходит взаимодействие между участниками.

Сценарий 1: Передача изделия происходит от участника A участнику B, желающему оставаться анонимным.

Шаг 1. Участник A располагает изделием с идентификатором itemId. Принадлежность изделия данному владельцу устанавливается с помощью вызова функции getItemHolder (itemId). Данная функция работает на чтение, поэтому транзакцию проводить в БД не нужно, достаточно иметь локальную копию актуальной версии БД. Отсутствие транзакции в БД важно для участника B, так как тот желает оставаться анонимным.

Шаг 3. Предоплата необходима для того, чтобы обезопасить A от пустой потери статуса владельца: на шаге 5, участник A фактически передает статус владельца B, но от B до сих пор не поступила полная оплата за изделие.

Шаги 4, 5. Участник A получает от B значение H_B, которое будет использовано для установки производного значения пароля на изделие. Участник A обладает предоплатой за изделие. Если A срывает сделку в данной точке, то B теряет свои деньги. Решить эту проблему можно, используя помощь надежного посредника.

Шаг 6. Прочитывая актуальную информацию из БД, участник B убеждается, что статус у изделия изменился, и что на изделие установили производное значение пароля, пароль которого известен только B. К данному моменту, у участника A уже нет

возможности вернуть себе статус владельца, а у участника B есть статус, но нет изделия, поэтому обе стороны мотивированы завершить сделку.

Сценарий 2: Передача изделия происходит между анонимным участником B и другим участником C, который также желает оставаться анонимным. Роль доверенного 3-го лица играет некоторый участник A, например, производитель изделий или иной субъект с возможностью проводить транзакции в БД.

Шаг 1. Участник B считывает публично известный ключ построения доказательств pk, формирует блок данных доказательства prf обладания паролем R_B, таким, что

$SHA256(R_B) = H_B$,

и передает это доказательство участнику C. Участник C получает из общедоступного места публично известный ключ проверки доказательств vk и производное значение пароля H_B для изделия, далее выполняет проверку

POC_VERIFY(SHA256(x), H_B, prf, vk) = Истина

Шаг 3. Предоплата нужна для того, чтобы после выполнения шага 6 (изменение производного значения пароля на новое значение), у участника C была мотивация к завершению сделки.

Шаг 4, 5. Для того, чтобы завершить сделку, B необходимо провести через A изменение производного значения пароля для изделия. Участник B не может сам вызвать эту транзакцию, так как потеряет анонимность. Поэтому, участник B обращается к производителю с запросом на вызов транзакции

changeHashKey(itemId, R_B, H_C).

Шаг 7. После проведения транзакции changeHashKey, участник B утратил доказательство обладания изделием, а C, наоборот, обладает таким доказательством. Участники мотивированы завершить сделку.

Сценарий 3. Передача изделия происходит между анонимным участником C и другим участником D, который также желает оставаться анонимным. Роль доверенного 3-го лица играет производитель изделий.

Шаг 1. Доказательство происходит аналогично сценарию 2.

Шаг 2. Предоплата нужна для того, чтобы после шага 3, у участника D была мотивация завершить сделку.

Шаги 3 и 4. Участник D получает официальный статус владельца изделием itemId.

Шаг 5. Участник D обладает статусом, но не изделием. У участников есть мотивация к тому, чтобы завершить сделку.

Сценарий 4: Передача изделия происходит между участником A и другим участником B, также желающим закрепить свой статус в БД.

Шаг 1. Предоплата нужна для того, чтобы у участника B была мотивация к завершению сделки после выполнения requestChangeHolder участником A на шаге 2. В смарт-контракте есть функция, позволяющая "отменить" передачу изделия cancelChangeHolder, но участник B может успеть вызвать ackChangeHolder до этого, и тогда A потеряет статус владения.

После этого оба участника мотивированы завершить сделку.

Под условием завершения сделки понимается совокупность действий и факторов, мотивирующих участников добросовестно следовать предложенному способу. Таким условием может быть частичная оплата (предоплата) за изделие до окончания сделки различными способами, использование услуг доверенного посредника и т.д. Предпочтительным вариантом является частичная оплата изделия после проверки его подлинности.

Таким образом, предложенный способ позволяет обеспечить возможности для покупателя остаться анонимным, даже при использовании БД типа публичный блокчейн.

Осуществление изобретения

Реализацию предложенного способа можно продемонстрировать на примере системы проверки подлинности драгоценных камней.

В качестве БД типа публичной блокчейн с поддержкой функции смарт-контрактов может быть выбрана блокчейн-платформа Ethereum (Блокчейн платформа Ethereum - статья по адресу https://www.ethereum.org) и ее общественная сеть Ethereum Mainnet (Обозреватель блоков основной сети Ethereum - статья по адресу https://etherscan.io/).

В качестве средства построения неинтерактивных доказательств с нулевым разглашением используется программная реализация алгоритмов zkSNARK под названием Zokrates (Библиотека ZoKrates для реализации криптографических схем неинтерактивных доказательств с нулевым разглашением - статья по адресу https://github.com/Zokrates/ZoKrates), способная по описанию вычислительной функции, оформленной на специальном языке, генерировать ключи pk, vk, а также функции построения доказательств POC_PROOF и проверки доказательств POC_VERIFY, в виде функций на языке Solidity (Язык программирования Solidity - статья по адресу https://www.solidity.readthedocs.io/en/v0.4.21/). Таким образом, эти функции могут быть записаны в БД и использованы внешними пользователями.

Производитель ценных изделий, например, драгоценных камней, создает ключевую пару, идентификатор в публичной БД Ethereum: в данном случае, идентификатором является значение хэш-функции от открытого ключа производителя; закрытый ключ сохраняется у производителя.

Производитель, используя средство построения неинтерактивных доказательств с нулевым разглашением и подавая в качестве параметра функцию A(x)=SHA256(x), получает два значения: pk - ключ построения доказательств и vk - ключ проверки доказательств, а также функции POC_PROOF и POC_VERIFY.

Производитель публикует ключи pk и vk, реализации функций POC_PROOF, POC_VERIFY, а также описание выбранной функции SHA256(x) в открытом доступе, например, на своем сайте в сети Интернет, или записывая в БД.

Производитель записывает в БД смарт-контракт, реализованный на языке программирования Solidity, выполненный с возможностью:

- вычислять функцию SHA256(x) (данная функция является встроенной для языка Solidity),
- добавлять изделие с идентификатором itemId в БД; в качестве владельца назначается идентификатор производителя изделий,
- инициировать процедуру передачи прав на изделие itemId от текущего владельца владельцу с идентификатором newHolder; для завершения процедуры передачи требуется, чтобы участник с идентификатором newHolder вызвал соответствующую функцию, таким образом подтвердив свое желание получить изделие во владение,
- подтверждать передачу изделия itemId во владение новым владельцем,
- отменить ранее инициированную процедуру передачи изделия
- считывать идентификатор владельца изделия с номером itemId,
- поставить значение текущего владельца для изделия с номером itemId в значение undefined (т.е. не определено), установив при этом производное значение пароля для данного изделия равным H,
- установить новое производное значение от пароля H для изделия itemId, предварительно предъявив пароль R, производное значение от которого равно текущему

установленному производному значению пароля для данного изделия,

● для изделия с идентификатором itemId, в случае, если текущий владелец изделия не выставлен (т.е. значение undefined), и, если производное значение переданного на вход пароля равно текущему производному значению пароля для изделия itemId, установить идентификатор текущего владельца равным newHolder.

При производстве драгоценности, изделию назначают уникальный идентификатор и наносят его на изделие, например, известным методом гравировки. После этого, записывают через смарт-контракт соответствие идентификатора изделия идентификатору производителя. Идентификатор производителя публично известен, например, опубликован на официальном сайте производителя. Таким образом, любой желающий может убедиться, что изделие было произведено данным производителем.

При покупке нового изделия, если покупатель желает закрепить свой статус владения в БД, то выполняют описанные в сценариях шаги. При этом, если у покупателя нет ключевой пары и соответствующей этой ключевой паре учетной записи в БД Ethereum, генерируют ключевую пару, например, используя приложение MetaMask (Приложение MetaMask - статья по адресу https://metamask.io/). Идентификатор учетной записи получается путем хэширования значения публичного ключа функцией SHA256.

Программное обеспечение, осуществляющее посылку транзакций в БД, можно реализовать, используя в качестве программной библиотеки - библиотеку web3.js или ethers.js (Библиотека web3.js - статья по адресу https://web3js.readthedocs.io/en/v1.2.4/; Библиотека Ethers.js - статья по адресу https://docs.ethers.io/ethers.js/html/), в качестве шлюза в блокчейн - сервис infura.io (Шлюз Infura.io - статья по адресу https://infura.io).

В некоторых сценариях пользователям требуется вычислить пароль и производное значение пароля. Пароль r и производное значение можно вычислить, используя стандартные программные средства: генератор псевдослучайных чисел, например, библиотеки random и hashlib языка программирования Python (Библиотека Random языка программирования Python - статья по адресу https://docs.python.org/3/library/random.html; Библиотека Hashlib языка программирования Python - статья по адресу https://docs.python.org/3/library/hashlib.html), позволяют это сделать. Важно, чтобы случайная величина r была равномерно распределена в диапазоне $1\ldots2^{256}$ для обеспечения достаточной устойчивости к атаке перебором.

Покупатель сохраняет выбранный пароль r в надежном месте, например, в долговременную память имеющегося у него вычислительного устройства.

Покупатель передает производно значение пароля h производителю. Осуществить это можно с помощью любого программного средства, реализующего функцию передачи сообщений с аутентификацией получателя.

Описанный в способе протокол реализуется с помощью указанных программных средств.

(57) Формула изобретения

1. Способ проверки подлинности изделий, реализуемый с использованием системы, содержащей

базу данных (БД) типа публичный блокчейн, связанную с сетью Интернет и выполненную с возможностью:

назначать идентификаторы пользователям БД;

осуществлять вызовы запрограммированных пользователями функций по управлению данными (смарт-контракт), которые способны выполнять следующие действия:

производить вычисление выбранной владельцем смарт-контракта функции A(x), где

x - натуральное число;

в случае, если изделие с заданным идентификатором отсутствует в БД, добавлять идентификатор изделия и указывать соответствие этого идентификатора изделия идентификатору производителя;

получать идентификатор владельца по заданному идентификатору изделия;

получать значение слепка пароля по заданному идентификатору изделия;

посылать запрос на изменение соответствия идентификатора изделия идентификатору текущего владельца на идентификатор нового владельца при наличии электронной цифровой подписи (ЭЦП) текущего владельца;

подтверждать изменение соответствия между идентификатором изделия и идентификатором владельца на соответствие идентификатору нового владельца при наличии ЭЦП нового владельца; отменять изменение соответствия идентификатора изделия идентификатору текущего владельца на идентификатор нового владельца при наличии ЭЦП текущего владельца;

изменять соответствие между идентификатором изделия и значением маски пароля с одновременным обнулением значения идентификатора текущего владельца изделия при наличии ЭЦП текущего владельца;

изменять соответствие между идентификатором изделия и производным значением пароля на новое производное значение пароля при предъявлении искомого действующего пароля изменять соответствие между идентификатором изделия и идентификатором владельца при наличии пароля r, значение от которого A(r) соответствует сохраненному ранее производному значению пароля;

добавлять смарт-контракты пользователей;

средство формирования доказательства вычисления без разглашения (далее СФДВ), выполненное с возможностью:

формировать ключ построения доказательства pk и ключ проверки доказательства vk с использованием функции A(x) в качестве параметра;

формировать блок данных доказательства Prf и численное значение b с использованием функции A(x) в качестве параметра, ключа формирования доказательств pk и численного значения d, причем A(d)=b;

верифицировать блок данных доказательства Prf с использованием функции A(x) в качестве параметра, ключа проверки доказательств vk и значения b;

получать и передавать данные;

способ заключается в том, что

выбирают функцию A(x), такую, что вычислительно трудно определить значение b по заданному значению c, причем A(b)=c;

формируют ЭЦП производителя;

назначают в БД уникальный идентификатор производителя;

формируют в СФДВ ключ проверки доказательства vk и ключ построения доказательств pk с использованием функции A(x);

формируют смарт-контракт в БД, содержащий функцию A(x), идентификатор производителя, значения ключа построения доказательств pk и ключа проверки доказательств vk;

если произведено новое изделие, то

назначают уникальный идентификатор изделию;

наносят назначенный идентификатор на изделие;

записывают в БД через смарт-контракт данные о соответствии идентификатора изделия идентификатору производителя; при необходимости передать изделие от

производителя покупателю,

формируют ЭЦП покупателя;

в случае, если покупатель желает закрепить свой статус владения в БД выполняют следующие действия:

если у покупателя отсутствует идентификатор в БД, назначают в БД уникальный идентификатор покупателю;

на стороне производителя, через смарт-контракт, посылают запрос на изменение соответствия идентификатора передаваемого изделия идентификатору покупателя, подписывая запрос ЭЦП производителя; на стороне покупателя, через смарт-контракт, подтверждают изменение соответствия между идентификатором передаваемого изделия и идентификатором покупателя, подписывая запрос ЭЦП покупателя; производят передачу изделия от производителя покупателю;

в случае, если покупатель желает остаться анонимным, выполняют следующие действия:

на стороне покупателя, производят проверку соответствия идентификатора изделия идентификатору производителя через БД;

на стороне покупателя, генерируют пароль r и вычисляют производное значение пароля h=A(r);

на стороне покупателя, сохраняют пароль r;

передают значение h от покупателя производителю;

на стороне покупателя, выполняют условие завершения сделки;

на стороне производителя, через смарт-контракт, изменяют соответствие идентификатора изделия производному значению пароля h, подписывая транзакцию ЭЦП производителя;

на стороне покупателя, через смарт-контракт, получают текущее значение производного значения пароля hp для передаваемого изделия если значение hp не равно h, то прерывают сделку;

производят передачу изделия от производителя покупателю;

при необходимости передать изделие от продавца покупателю,

формируют ЭЦП покупателя;

формируют ЭЦП продавца;

в случае, если соответствие идентификатора передаваемого изделия идентификатору продавца зафиксировано в БД, и покупатель желает также закрепить свой статус владения в БД, то выполняют следующие действия:

если у покупателя отсутствует идентификатор в БД, назначают уникальный идентификатор покупателю в БД;

на стороне продавца, через смарт-контракт, формируют запрос на изменение соответствия идентификатора передаваемого изделия идентификатору покупателя, подписывая запрос ЭЦП продавца;

на стороне покупателя, через смарт-контракт, подтверждают изменение соответствия идентификатора изделия идентификатору покупателя, подписывая транзакцию ЭЦП покупателя;

производят передачу изделия от продавца покупателю;

в случае, если соответствие идентификатора передаваемого изделия идентификатору продавца зафиксировано в БД, а покупатель желает остаться анонимным, то выполняют следующие действия:

проверяют подлинность изделия путем сравнения идентификатора текущего владельца передаваемого изделия, записанного в БД и идентификатора продавца;

если идентификаторы не совпали, то прерывают сделку;

на стороне покупателя, генерируют пароль r1 и вычисляют производное значение пароля h1=A(r1);

сохраняют пароль r1 на стороне покупателя;

передают значение h1 от покупателя продавцу;

на стороне покупателя, выполняют условие завершения сделки;

на стороне продавца, в смарт-контракте, меняют соответствие между идентификатором изделия и производным значением пароля на новое значение h1, подписывая транзакцию с помощью ЭЦП продавца;

на стороне покупателя, через смарт-контракт, получают текущее производное значение пароля h2, соответствующее идентификатору передаваемого изделия;

если значение h2 не равно h1, то прерывают сделку;

производят передачу изделия от продавца покупателю;

в случае, если соответствие идентификатора передаваемого изделия идентификатору продавца не зафиксировано в БД, и покупатель желает остаться анонимным, то выполняют следующие действия:

на стороне продавца, запрашивают из смарт-контракта ключ построением доказательств pk;

на стороне продавца, используя СФДВ, формируют блок доказательства prf2 с использованием функции A(x), пароля r, сохраненного на стороне продавца, и ключа построения доказательств pk;

передают блок доказательства prf2 от продавца покупателю; на стороне покупателя, запрашивают из БД ключ проверки доказательств vk;

на стороне покупателя, через смарт-контракт, получают производное значение пароля h, соответствующее передаваемому изделию;

на стороне покупателя, используя СФДВ, производят проверку блока доказательства prf2 с использованием функции A(x), производного значения пароля h и ключа vk;

если проверка неуспешна, то прерывают сделку;

на стороне покупателя, формируют пароль r2;

на стороне покупателя, вычисляют производное значение пароля h2=A(r2);

на стороне покупателя, сохраняют пароль r2;

отправляют значение h2 от покупателя продавцу;

на стороне покупателя, выполняют условие завершения сделки;

на стороне продавца, отправляют производителю запрос на изменение соответствия идентификатора изделия новому производному значению пароля h2, передавая текущий пароль r;

на стороне производителя, через смарт-контракт меняют соответствие между идентификатором передаваемого изделия и производным значением пароля на новое значение h2, предъявляя текущий пароль r и подписывая транзакцию ЭЦП производителя;

если покупатель устанавливает, что производное значение пароля для передаваемого изделия не изменилось в БД, или изменилось, но не равно h2, то прерывают сделку;

производят передачу изделия от продавца покупателю;

в случае, если соответствие идентификатора передаваемого изделия идентификатору продавца не зафиксировано в БД, а покупатель желает закрепить свой статус владения в БД, то выполняют следующие действия:

если у покупателя отсутствует идентификатор в БД, назначают уникальный идентификатор покупателю;

если у покупателя отсутствует ЭЦП, формируют ЭЦП покупателя; на стороне продавца, в смарт-контракте, запрашивают ключ построения доказательства pk;

на стороне продавца, используя СФДВ, формируют блок данных доказательства prf3, используя в качества параметров функцию A(x), ключ построения доказательств pk и пароля r3;

производят передачу блока доказательства prf3 от продавца покупателю;

на стороне покупателя, в смарт-контракте, запрашивают ключ проверки доказательства vk;

на стороне покупателя, в смарт-контракте, запрашивают производное значение от пароля h3, соответствующую передаваемому изделию;

на стороне покупателя, используя СФДВ, производят проверку блока доказательства, используя в качестве параметров функцию A(x), ключ проверки доказательств vk, производное значение от пароля h3 и блок данных доказательства prf3;

если проверка неуспешна, то прерывают сделку; на стороне покупателя, выполняют условие завершения сделки; передают пароль r3 от продавца покупателю;

на стороне покупателя, через смарт-контракт, меняют соответствие идентификатора изделия идентификатору покупателя, используя переданный пароль r3;

передают изделие от продавца покупателю.

2. Способ по п. 1, в котором в качестве функции A(x) выбирают криптографическую хэш-функцию.