РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 679 545**(13) **C1**

(51) МПК
G06F 16/21 (2019.01)
G06Q 30/06 (2012.01)
G06K 5/02 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 17/30 (2018.08); G06Q 30/06 (2018.08); G06K 5/02 (2018.08)

(21)(22) Заявка: **2018115086, 24.04.2018**

(24) Дата начала отсчета срока действия патента:
24.04.2018

Дата регистрации:
11.02.2019

Приоритет(ы):
(22) Дата подачи заявки: **24.04.2018**

(45) Опубликовано: **11.02.2019** Бюл. № **5**

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 2643503 C1, 01.02.2018. RU 2639015 C1, 19.12.2017. WO 2018/064329 A1, 05.04.2018. WO 2018/064645 A1, 05.04.2018.**

(54) Способ проверки подлинности изделий

(57) Реферат:

Изобретение относится к способу проверки подлинности изделия. Техническим результатом является снижение транзакционных издержек, повышение производительности процедуры передачи изделий. 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.

RU 2679545 C1

RU 2679545 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 679 545**(13) **C1**

(51) Int. Cl.
G06F 16/21 (2019.01)
G06Q 30/06 (2012.01)
G06K 5/02 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 17/30 (2018.08); G06Q 30/06 (2018.08); G06K 5/02 (2018.08)

(21)(22) Application: **2018115086, 24.04.2018**

(24) Effective date for property rights:
24.04.2018

Registration date:
11.02.2019

Priority:
(22) Date of filing: **24.04.2018**

(45) Date of publication: **11.02.2019** Bull. № **5**

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 2679545 C1

(54) PRODUCTS AUTHENTICITY VERIFICATION METHOD

(57) Abstract:

FIELD: testing equipment.

SUBSTANCE: invention relates to the product authenticity verification method. Method is implemented using the system containing a public blockchain type database (DB) connected to the Internet and configured to assign identifiers to the DB users; make calls of the programmed by users data management functions (smart contract), which are able to perform the following actions: in case if the product with the specified identifier is missing in the DB, add the product identifier and indicate this product identifier compliance with the manufacturer identifier; change the correspondence between the product identifier and the owner identifier in the presence of a digital signature (EDS) from the current product owner and the new owner EDS; change the correspondence between the product identifier and the owner identifier with the transactions between chain owners the specification with all of the intermediate owners correct EDS indication; add the users smart-contracts; wherein at the next product transfer, the current owner sends the signed by its signature transaction directly to the next owner, avoiding the need to make the transaction into the blockchain.

EFFECT: technical result is reduction in the transaction costs, increase in the products transferring procedure productivity.

1 cl

RU 2679545 C1

Область техники, к которой относится изобретение

Предлагаемое 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 них:

1) нанесение на изделие специальных отличительных голографических наклеек (патент РФ №2242802, приоритет от 17.04.2003 г.);

2) нанесение на изделие специального идентифицирующего кода, с возможностью проверки в общедоступной базе данных соответствия этого кода данному изделию (патент РФ №2225032, приоритет от 18.10.2002 г.);

3) нанесение RFID-меток (патент РФ №2292587, приоритет от 21.06.2005 г.);

4) запись идентификатора изделия и идентификатора текущего владельца в базу данных (БД) типа блокчейн (патент РФ №2639015, приоритет от 26.01.2017 г.; патент РФ №2643503, приоритет от 12.05.2017 г.).

Недостатком способа с использованием голографических наклеек является сложность проверки таких наклеек на подлинность; требуется специальное оборудование, зачастую недоступное широкому потребителю, это затрудняет применение способа.

Недостатком способа с использованием идентифицирующего кода является то, что при получении злоумышленником хотя бы одного достоверного идентификатора изделия, ничто не мешает произвести копии с таким же идентификатором. Это существенно сужает область применимости способа.

Недостатком способа с использованием RFID-меток является необходимость иметь специальное оборудование, как для производства меток, так и для их проверки. Такое оборудование зачастую недоступно широкому потребителю, что затрудняет применение способа.

Способ с использованием записи информации об изделии и текущем владельце в БД типа блокчейн представляется наиболее перспективным. Данный способ имеет ряд преимуществ по сравнению с другими способами отслеживания подлинности изделия: помимо идентификатора самого изделия, в публично доступной 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.

Возможна ситуация, при которой владелец подлинного изделия передает контрафактное изделие под видом подлинного. Но делать это ему нет экономического смысла - после передачи контрафактного изделия запись о владении изделием будет изменена на следующего владельца, таким образом, подлинное изделие, оставшееся на руках у продавца, потеряет свой законный статус, что неизменно скажется на его стоимости в сторону уменьшения.

Еще одним аргументом в пользу такого вида БД является ее свойства неизменяемости: даже производитель изделий не сможет подменить информацию о владельце ни умышленно, ни ошибочно, таким образом доверие к ней выше, чем у традиционных БД.

Дополнительным аргументом является то, что БД типа блокчейн обладают свойством высокой доступности, таким образом, она не подвержена DDoS-атакам.

На данный момент известен проект EverLedger (Проект EverLedger, информация по адресу https://www.everledger.io/#technology), который реализует систему контроля подлинности драгоценных изделий на базе технологии блокчейн. Однако, помимо того, что система существует и действует, информации о ее техническом устройстве в публичном доступе нет.

Известен способ проверки подлинности товаров или услуг (патент РФ №2643503, приоритет от 12.05.2017 г.), опирающийся на технологию блокчейн. Техническим результатом описываемого способа является возможность настройки прав доступа к данным, сохраняемым в БД о товарах или услугах. Идея способа заключается в том, что не все данные о товаре должны быть общедоступны; при этом часть данных должна быть доступна только уполномоченным лицам (например, регулирующим органам), а остальная часть данных доступна рядовому покупателю.

Одна из возможных реализаций подобного способа известна (Погружение в технологию блокчейн: борьба с контрафактными товарами, статья по адресу https://habrahabr.ru/company/microsoft/blog/312054/), предложен способ, в котором:

- при производстве изделия, назначают уникальный идентификатор изделию;
- наносят на изделие назначенный идентификатор;
- ставят в соответствие идентификатору изделия публично известный идентификатор изготовителя, 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. Известный способ принят за прототип. Однако, известный способ имеет недостатки.

Одним из них можно указать высокие транзакционные издержки. При передаче большого количества изделий, например, партию, необходимо производить большое количество транзакций, что связано с ощутимыми затратами.

Другим недостатком является необходимость потенциально долгого ожидания внесения записи транзакции в блок при каждой передаче.

Раскрытие изобретения

Техническим результатом предлагаемого изобретения является

1) снижение транзакционных издержек для участников цепочки владения,

2) повышение производительности процедуры передачи изделий,

Для этого предлагается способ проверки подлинности изделия, 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

- 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 наличие 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; способ заключается в том, что
- назначают уникальный идентификатор производителю в БД;
- формируют смарт-контракт в БД, содержащий идентификатор производителя;
- если произведено новое изделие, то

○ назначают уникальный идентификатор изделию; ○ наносят назначенный идентификатор на изделие;

○ записывают в БД посредством смарт-контракта данные о соответствии идентификатора изделия идентификатору производителя; при необходимости передать изделие от производителя новому владельцу,

- если у нового владельца отсутствует идентификатор в БД, назначают уникальный идентификатор новому владельцу;
- формируют транзакцию на передачу изделия от производителя новому владельцу, указывая идентификатор изделия, идентификатор производителя, идентификатор нового владельца;
- подписывают сформированную транзакцию ЭЦП производителя;
- отправляют сформированную транзакцию новому владельцу;
- проверяют правильность указания идентификаторов производителя, нового владельца и изделия; если какой-либо из идентификаторов указан неверно, то прерывают сделку;
- проверяют корректность ЭЦП производителя; если проверка прошла неуспешно, то прерывают сделку;
- проверяют соответствие идентификатора изделия идентификатору производителя в БД; если проверка прошла неуспешно, то прерывают сделку;
- производят передачу изделия от производителя новому владельцу;
- подписывают транзакцию ЭЦП нового владельца;
- если изделие не планируется более передавать в ближайшее время, то записывают транзакцию в БД посредством смарт-контракта, иначе сохраняют полученную транзакцию у нового владельца;

при необходимости передать изделие от текущего владельца новому владельцу, в случае, если факт владения изделием текущим владельцем зафиксирован в БД,

- формируют транзакцию на передачу изделия от текущего владельца новому

владельцу, указывая идентификатор изделия, идентификатор текущего владельца, идентификатор нового владельца;

- подписывают сформированную транзакцию ЭЦП текущего владельца;
- отправляют сформированную транзакцию новому владельцу;
- проверяют корректность ЭЦП текущего владельца; если проверка прошла неуспешно, то прерывают сделку;
- проверяют соответствие идентификатора изделия идентификатору текущего владельца, если проверка прошла неуспешно, то прерывают сделку;
- производят передачу изделия от текущего владельца новому владельцу;
- подписывают транзакцию ЭЦП нового владельца;
- если изделие не планируется более передавать в ближайшее время, то записывают транзакцию в БД посредством смарт-контракта, иначе сохраняют полученную транзакцию у нового владельца;

при необходимости передать изделие от текущего владельца новому владельцу, в случае, если факт владения изделием текущим владельцем не зафиксирован в БД,

- формируют расширенную транзакцию на передачу изделия от текущего владельца новому владельцу, указывая
  - идентификатор изделия;
  - идентификатор текущего владельца, идентификатор нового владельца;
  - всю цепочку предыдущих транзакций передач от идентификатора владельца, зафиксированного в базе данных, вплоть до текущего владельца;
- подписывают расширенную транзакцию ЭЦП текущего владельца;
- отправляют расширенную транзакцию новому владельцу;
- проверяют корректность ЭЦП всех владельцев из цепочки транзакций в составе расширенной транзакции; если проверка прошла неуспешно, то прерывают сделку;
- производят передачу изделия от текущего владельца новому владельцу;
- подписывают расширенную транзакцию ЭЦП нового владельца;
- если изделие не планируется более передавать в ближайшее время, записывают расширенную транзакцию в БД посредством смарт-контракта, иначе сохраняют расширенную транзакцию.

При очередной передаче изделия текущий владелец посылает подписанную своей подписью транзакцию напрямую следующему владельцу, избегая необходимости производить транзакцию в блокчейн. Это позволяет избежать транзакционных и временных издержек при передаче изделия.

В настоящее время средняя стоимость транзакции составляет порядка 0.7 USD, а время подтверждения транзакции в блокчейн сети Ethereum составляет в среднем 10 секунд (Блокчейн платформа Ethereum, информация по адресу www.ethereum.org). В случае, если требуется выполнить записи в отношении множества изделий (партии), издержки могут стать значительными.

Несмотря на то, что транзакция о факте передачи изделия не отправляется в блокчейн, в любой момент времени у нового владельца имеются доказательства владения: вся цепочка подписанных передач, от производителя, и до текущего владельца. В случае, если новый владелец желает закрепить свой статус владения в блокчейне, он посылает

расширенную транзакцию в смарт-контракт; в расширенной транзакции зафиксированы все промежуточные передачи, которые имели место, начиная от последнего владельца, зафиксированного в блокчейне, и до текущего владельца.

Можно отметить, что, если производитель реализовал предлагаемый способ, у злоумышленников остается немного мотивации к производству контрафактной продукции, отнесенной к данному производителю. Поскольку процедура установки соответствия владельца и уникального идентификатора изделия зафиксированы в неизменяемом доступном для изучения смарт-контракте в БД типа блокчейн, любой покупатель может, имея доступ в сеть Интернет, достоверно проверить подлинность изделия. Если в блокчейне не значится идентификатор передаваемого изделия, то оно однозначно контрафактное, так как производитель не производил изделие с таким идентификатором. Если в блокчейне идентификатор изделия закреплен за другим владельцем, и текущий владелец не обладает доказательством передачи изделия от предыдущего владельца, значит изделие либо незаконно приобретенное, либо контрафактное, что значительно затруднит его сбыт.

Возможен сценарий, при котором злоумышленник приобретает подлинное изделие с целью производства его контрафактных копий. Если при продаже контрафактного изделия злоумышленник убеждает нового владельца не отправлять транзакцию в блокчейн и не закреплять свой статус владельца, у злоумышленника остается возможность повторной продажи контрафактной копии изделия до того момента, пока новый владелец не отправит транзакцию в смарт-контракт.

На практике, однако, такое развитие событий маловероятно: в случае, если изделие штучное и дорогостоящее, например, такое, как драгоценный камень или картина, с большой долей вероятности очередной покупатель захочет закрепить свой статус в блокчейне в момент передачи, и тем самым помешает злоумышленнику продавать контрафактные копии.

Если происходит продажа менее дорогостоящего изделия, например, часов, то, в этом случае, экономически оправданным для злоумышленника может стать только массовая продажа контрафактных копий изделия, а это вряд ли получится, так как с каждым новым покупателем вероятность того, что тот зафиксирует статус владельца в блокчейне, увеличивается.

С учетом этого, предложенный способ, несмотря на наличие возможности внести контрафакт в цепочку, тем не менее, на практике значительно затрудняет массовой выпуск контрафактных копий.

Осуществление изобретения

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

Производитель драгоценностей создает идентификатор в публичной блокчейн БД Ethereum ((Блокчейн платформа Ethereum, информация по адресу www.ethereum.org)): в данном случае, идентификатором является хэш-значение от публичного ключа; приватный ключ сохраняется у производителя.

Производитель записывает в блокчейн смарт-контракт, реализованный на языке программирования Solidity (Язык программирования Solidity, информация по адресу solidity.readthedocs.io/en/v0.4.21/), выполненный с возможностью:

- добавлять новые изделия в БД, в случае, если изделие с заданным идентификатором до сих пор не было добавлено;
- назначать соответствие идентификатору изделия идентификатор владельца, при условии наличия ЭЦП текущего владельца и нового владельца;

- изменять соответствие между идентификатором изделия и идентификатором владельца, при указании цепочки транзакций между владельцами, с указанием корректных ЭЦП всех промежуточных владельцев.

При производстве драгоценности, изделию назначают уникальный идентификатор и наносят его на изделие, например, известным методом гравировки.

Затем записывают 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 продаже изделия, в случае, если у покупателя отсутствует идентификатор в блокчейне Ethereum, создают уникальный идентификатор покупателю.

Производитель формирует транзакцию, в которой указывает идентификатор передаваемого изделия, покупателя и производителя; подписывает транзакцию собственной ЭЦП и отправляет покупателю. Покупатель производит проверку корректности заполнения полей и, в случае успешной проверки, подписывает транзакцию собственной ЭЦП. В зависимости от дальнейших намерений нового владельца (покупателя), может быть сделано следующее:

- если изделие не планируется в ближайшее время передавать другому лицу, записывают сформированную транзакцию в блокчейн, используя смарт-контракт производителя; таким образом, соответствие между идентификатором данного изделия и идентификатором владельца будет надежно зафиксировано;
- если изделие планируется в ближайшее время передавать другому лицу, либо, если происходит передача сразу большого количества изделий, то можно не производить транзакцию, а сохранить ее у нового владельца на каком-либо носителе для возможности подтвердить свое право владения изделием в будущем, без необходимости проводить транзакцию в блокчейн.

При осуществлении очередной передачи изделия между текущим владельцем и новым владельцем, в случае, если соответствие между идентификатором изделия и идентификатором текущего владельца не было зафиксировано в блокчейне, делают следующее:

- если у нового владельца отсутствует идентификатор в блокчейне, создают уникальный идентификатор (ключевая пара);
- создают сетевое соединение между текущим владельцем и новым владельцем;
- формируют на стороне текущего владельца расширенную транзакцию, в которой указывают идентификатор текущего владельца, идентификатор нового владельца, идентификатор изделия, а также указывают сохраненную ранее транзакцию в качестве доказательства передачи изделия от производителя текущему владельцу;
- подписывают сформированный блок данных ЭЦП текущего владельца;
- отправляют расширенную транзакцию по сетевому соединению новому владельцу;
- на стороне нового владельца проверяют правильность заполнения полей, корректность ЭЦП текущего владельца и корректность транзакции, подтверждающей переход изделия от производителя текущему владельцу;
- в случае, если какая-либо из проверок прошла неуспешно, прерывают сделку;
- проводят передачу изделия от текущего владельца новому владельцу;

- подписывают полученную транзакцию ЭЦП нового владельца;
- сохраняют транзакцию у нового владельца, либо отправляют ее в блокчейн, в смарт-контракт производителя.

В качестве алгоритма ЭЦП может использоваться алгоритм ECDSA с эллиптической кривой secp256k1. Данный алгоритм позволяет узнать публичный ключ подписавшей стороны, если известна подписываемая информация.

Программный модуль, реализующий формирование транзакции при передаче изделия от владельца к владельцу по прямому информационному каналу, может быть реализован на любом языке программирования общего назначения, например на языке Python (Язык программирования Python, информация по адресу www.python.org).

При очередной передаче изделия, текущий владелец посылает подписанную своей ЭЦП транзакцию напрямую следующему владельцу, избегая необходимости производить транзакцию в блокчейн. Это позволяет избежать транзакционных издержек на оплату транзакции и ожидания включения транзакции в блок.

Несмотря на то, что транзакция не была отправлена в блокчейн, в любой момент времени у нового владельца имеются доказательства владения: вся цепочка подписанных передач, от производителя, и до текущего владельца.

Затруднение появления контрафактных копий достигается за счет того, что попытка передать изделие с указанным на нем идентификатором позволяет проверить в БД соответствие между идентификатором текущего владельца и идентификатором передаваемого изделия.

При несовпадении идентификатора передающей стороны тому, что указано в БД, приводит к прерыванию сделки. Способ предполагает также возможность предъявить доказательства владения помимо БД, по прямому информационному каналу. Но сделать это может только подлинный владелец, так как каждая передача заверяется ЭЦП передающей стороны, которая берет начало от производителя.

(57) Формула изобретения

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:

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;

способ заключается в том, что

назначают уникальный идентификатор производителю в БД;

формируют смарт-контракт в БД, содержащий идентификатор производителя;

если произведено новое изделие, то

назначают уникальный идентификатор изделию;

наносят назначенный идентификатор на изделие;

записывают в БД посредством смарт-контракта данные о соответствии идентификатора изделия идентификатору производителя;

при необходимости передать изделие от производителя новому владельцу,

если у нового владельца отсутствует идентификатор в БД, назначают уникальный идентификатор новому владельцу;

формируют транзакцию на передачу изделия от производителя новому владельцу, указывая идентификатор изделия, идентификатор производителя, идентификатор нового владельца;

подписывают сформированную транзакцию ЭЦП производителя;

отправляют сформированную транзакцию новому владельцу;

проверяют правильность указания идентификаторов производителя, нового владельца и изделия; если какой-либо из идентификаторов указан неверно, то прерывают сделку;

проверяют корректность ЭЦП производителя; если проверка прошла неуспешно, то прерывают сделку;

проверяют соответствие идентификатора изделия идентификатору производителя в БД; если проверка прошла неуспешно, то прерывают сделку;

производят передачу изделия от производителя новому владельцу;

подписывают транзакцию ЭЦП нового владельца;

если изделие не планируется более передавать в ближайшее время, то записывают транзакцию в БД посредством смарт-контракта, иначе сохраняют полученную транзакцию у нового владельца;

при необходимости передать изделие от текущего владельца новому владельцу, в случае если факт владения изделием текущим владельцем зафиксирован в БД,

формируют транзакцию на передачу изделия от текущего владельца новому владельцу, указывая идентификатор изделия, идентификатор текущего владельца, идентификатор нового владельца;

подписывают сформированную транзакцию ЭЦП текущего владельца;

отправляют сформированную транзакцию новому владельцу;

проверяют корректность ЭЦП текущего владельца; если проверка прошла неуспешно, то прерывают сделку;

проверяют соответствие идентификатора изделия идентификатору текущего владельца; если проверка прошла неуспешно, то прерывают сделку;

производят передачу изделия от текущего владельца новому владельцу;

подписывают транзакцию ЭЦП нового владельца;

если изделие не планируется более передавать в ближайшее время, то записывают транзакцию в БД посредством смарт-контракта, иначе сохраняют полученную транзакцию у нового владельца;

при необходимости передать изделие от текущего владельца новому владельцу, в случае если факт владения изделием текущим владельцем не зафиксирован в БД,

формируют расширенную транзакцию на передачу изделия от текущего владельца новому владельцу, указывая

идентификатор изделия;

идентификатор текущего владельца, идентификатор нового владельца;

всю цепочку предыдущих транзакций передач от идентификатора владельца, зафиксированного в базе данных, вплоть до текущего владельца;

подписывают расширенную транзакцию ЭЦП текущего владельца;

отправляют расширенную транзакцию новому владельцу;

проверяют корректность ЭЦП всех владельцев из цепочки транзакций в составе расширенной транзакции; если проверка прошла неуспешно, то прерывают сделку;

производят передачу изделия от текущего владельца новому владельцу;

подписывают расширенную транзакцию ЭЦП нового владельца;

если изделие не планируется более передавать в ближайшее время, записывают расширенную транзакцию в БД посредством смарт-контракта, иначе сохраняют расширенную транзакцию.