

# ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ



НАЦИОНАЛЬНЫЙ ЦЕНТР  
ИНТЕЛЛЕКТУАЛЬНОЙ  
СОБСТВЕННОСТИ

(19) ВУ (11) 23492

(13) С1

(46) 2021.08.30

(51) МПК

G 06Q 20/00 (2012.01)

## (54) СПОСОБ И СИСТЕМА ВЫПОЛНЕНИЯ ТРАНЗАКЦИЙ ПО ПЕРЕДАЧЕ ЦИФРОВЫХ АКТИВОВ

(21) Номер заявки: а 20180092  
(22) 2017.06.21  
(31) а 201704103 (32) 2017.04.25 (33) UA  
(85) 2019.11.25  
(86) PCT/UA2017/000068, 2017.06.21  
(87) WO 2017/196289, 2017.11.16  
(43) 2020.02.28  
(71) Заявитель: Общество с ограниченной ответственностью "Симкорд" (UA)  
(72) Автор: КУДЬ, Александр (UA)

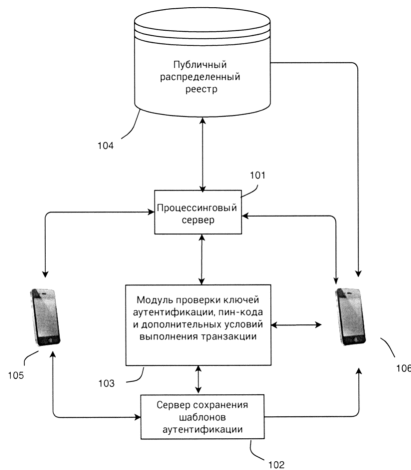
(73) Патентообладатель: Общество с ограниченной ответственностью "Симкорд" (UA)  
(56) US 2016/0071097 A1.  
BY 5166 U, 2009.  
BY 7736 C1, 2006.  
RU 2599951 C2, 2016.  
RU 2145438 C1, 2000.

(57)

1. Способ выполнения транзакции по передаче цифрового актива, при котором направляют посредством коммуникационного устройства плательщика запрос транзакции на процессинговый сервер системы выполнения транзакций по передаче цифровых активов;

вводят в систему посредством коммуникационного устройства плательщика номинал передаваемого цифрового актива, имя и параметры аутентификации его получателя, тип, пин-код и основные условия выполнения транзакции и сохраняют указанные введенные данные на сервере сохранения шаблонов аутентификации указанной системы;

вводят в систему и сохраняют на сервере сохранения шаблонов аутентификации выбранные плательщиком дополнительные условия выполнения транзакции;



Фиг. 1

ВУ 23492 С1 2021.08.30

## ВУ 23492 С1 2021.08.30

создают первичный ключ аутентификации в виде содержащего метаданные графического изображения заданного физического объекта либо серии таких изображений путем фотосъемки указанного объекта коммуникационным устройством плательщика и сохраняют указанный ключ на сервере сохранения шаблонов аутентификации;

сохраняют в публичном распределенном реестре информацию о запланированной транзакции, после чего блокируют в учетной записи плательщика передаваемый цифровой актив;

информируют получателя о физическом объекте, использованном для создания первичного ключа аутентификации, и обо всех указанных данных, необходимых для выполнения транзакции;

направляют посредством коммуникационного устройства получателя запрос транзакции на процессинговый сервер;

вводят в систему посредством коммуникационного устройства получателя тип и пин-код транзакции, информацию о соблюдении указанных условий ее выполнения, а также первичный ключ аутентификации, воспроизведенный получателем с использованием того же физического объекта;

устанавливают подлинность всех введенных получателем данных путем их сравнения с теми же данными, ранее сохраненными плательщиком на сервере сохранения шаблонов аутентификации;

после чего списывают заблокированный актив с учетной записи плательщика, зачисляют его на учетную запись получателя, удаляют с сервера сохранения шаблонов аутентификации использованный первичный ключ аутентификации и сохраняют информацию о выполненной транзакции в публичном распределенном реестре.

2. Способ по п. 1, **отличающийся** тем, что в качестве дополнительных условий выполнения транзакции используют желаемую дату ее выполнения.

3. Способ по п. 1, **отличающийся** тем, что в качестве дополнительных условий выполнения транзакции используют данные о желаемом диапазоне дат ее выполнения.

4. Способ по п. 1, **отличающийся** тем, что в качестве дополнительных условий выполнения транзакции используют данные о географическом местоположении получателя.

5. Способ по п. 1, **отличающийся** тем, что после направления плательщиком запроса транзакции дополнительно создают вторичный ключ аутентификации, сохраняют его на сервере сохранения шаблонов аутентификации и информируют о нем получателя, а после направления запроса получателем вводят в систему воспроизведенный получателем вторичный ключ аутентификации, после чего сравнивают его с тем же ключом, ранее сохраненным плательщиком на сервере сохранения шаблонов аутентификации.

6. Способ по п. 5, **отличающийся** тем, что в качестве вторичного ключа аутентификации используют содержащую метаданные аудиозапись.

7. Способ по п. 5, **отличающийся** тем, что в качестве вторичного ключа аутентификации используют содержащую метаданные видеозапись.

8. Способ по п. 5, **отличающийся** тем, что в качестве вторичного ключа аутентификации используют содержащий метаданные текстовый файл.

9. Способ по п. 1, **отличающийся** тем, что в качестве имени получателя вводят в систему указание на анонимного получателя.

10. Система выполнения транзакций по передаче цифровых активов способом по п. 1, содержащая взаимосвязанные

по меньшей мере один процессинговый сервер, выполненный с возможностью получения с коммуникационных устройств плательщика и получателя запросов транзакций, а также с возможностью списывания активов с учетной записи плательщика и их зачисления на учетную запись получателя;

сервер сохранения шаблонов аутентификации, выполненный с возможностью сохранения и удаления введенных в систему номиналов передаваемых цифровых активов, име-

ни и параметров аутентификации получателя, типов, пин-кодов и условий выполнения транзакций, а также первичных ключей аутентификации, созданных в виде графических изображений заданного физического объекта, содержащих метаданные, либо серий таких изображений;

модуль проверки, выполненный с возможностью установления подлинности всех введенных получателем в систему данных транзакции путем их сравнения с теми же данными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации; публичный распределенный реестр данных о транзакциях.

11. Система по п. 10, **отличающаяся** тем, что модуль проверки выполнен с возможностью сравнения аудиозаписей и их метаданных, введенных получателем, с такими же аудиозаписями и их метаданными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации.

12. Система по п. 10, **отличающаяся** тем, что модуль проверки выполнен с возможностью сравнения видеозаписей и их метаданных, введенных получателем, с такими же видеозаписями и их метаданными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации.

13. Система по п. 10, **отличающаяся** тем, что модуль проверки выполнен с возможностью сравнения текстовых файлов и их метаданных, введенных получателем, с такими же файлами и их метаданными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации.

14. Система по п. 10, **отличающаяся** тем, что модуль проверки выполнен с возможностью сравнения желаемой даты осуществления транзакции, сохраненной плательщиком, с текущей датой транзакции.

15. Система по п. 10, **отличающаяся** тем, что модуль проверки выполнен с возможностью сравнения данных о желаемом географическом местоположении получателя, сохраненных плательщиком, с данными о текущем местоположении получателя.

16. Система по п. 10, **отличающаяся** тем, что указанный реестр выполнен в виде сети взаимосвязанных аппаратно-программных комплексов.

---

Заявленное изобретение касается информационных технологий и предназначено для использования в финансовой сфере, управлении правами на цифровые ценности, передаче прав на цифровые активы. Изобретение может быть использовано компаниями, предпринимателями и обычными физическими лицами.

С развитием и глобальным распространением платежных систем безналичные расчеты между обычными людьми также получили глобальное распространение. Например, типична ситуация, когда один человек на сайте объявлений находит информацию о продаже товара другим человеком и осуществляет безналичную оплату на карточный счет продавца.

Распространена ситуация, когда один человек безналичным переводом пополняет карточный счет другого человека с целью осуществить оплату любой услуги, которую тот ему оказывает (например, уборка в доме, присмотр за ребенком, выгул собаки).

Также типичной является ситуация, когда родители безналичным способом переводят деньги своему ребенку, пополняя его карточный счет. Или, наоборот, взрослые дети безналичным способом пополняют карточный счет своих родителей, оказывая им финансовую помощь.

Все чаще встречается ситуация, когда для расчетов между людьми используются стоимостные эквиваленты денежных единиц (электронные деньги, цифровые активы и другие цифровые ценности). При этом такие расчеты осуществляют с использованием компьютерных и/или сотовых сетей операторов связи без обращения к традиционным финансовым учреждениям, таким как банки или платежные системы.

Во всех этих случаях могут быть использованы предложенный способ выполнения транзакции по передаче цифровых активов и система для его реализации. Необходимо указать, что перечисленные случаи не ограничивают сферу использования заявленных способа и системы.

Известен способ выполнения платежных транзакций, который предусматривает инициирование плательщиком запроса в платежную систему на осуществление платежной транзакции в пользу получателя, ввод плательщиком в платежную систему номинала платежа, названия получателя, адреса получателя, сохранение в платежной системе названия получателя, номинала платежа, адреса получателя, создание платежной системой кода транзакции и сообщение его плательщику, сообщение плательщиком получателю номинала транзакции и кода аутентификации, создание получателем запроса в платежную систему на получение платежа, ввод в платежную систему получателем кода транзакции, проверку платежной системой кода транзакции, выполнение транзакции при успешной проверке или отмену транзакции при неуспешной проверке [см. описание системы Western Union на сайте <https://www.westernunion.com/us/en/home.html>].

Способ предназначен для выполнения транзакций с наличными и безналичными средствами. Аутентификация получателя осуществляется по его персональным данным и по коду транзакции. Недостатком способа является отсутствие возможности выполнять транзакции с другими, кроме денег, активами. Кроме того, способ требует обязательного указания названия получателя и его адреса и не позволяет выполнять транзакции в пользу анонимных получателей. К недостаткам способа также можно отнести невозможность указания плательщиком условий выполнения транзакции (даты, географического места).

Известен способ выполнения платежных транзакций, предусматривающий получение от получателя счета на оплату, выявление на счете графического изображения (подпись или логотип), который идентифицирует получателя, идентификацию получателя путем распознавания имеющихся в системе подписей и логотипов известных получателей, выполнение предназначенного для идентифицированного получателя правила оплаты. Система, предназначенная для осуществления этого способа, содержит сервер для обработки данных, сервер хранения данных о получателях и данных о правилах оплаты, факс-сервер [заявка на патент US 20130226798, МПК G 06Q 20/10, G 06Q 20/40, дата публикации 29.08.2013].

Известная система ориентирована на автоматизацию работы со счетами на оплату, полученными плательщиком от получателей, и не предназначена для обслуживания транзакций, созданных по инициативе плательщика. Система не в состоянии выполнять транзакции в пользу получателей, сведения о которых заранее не внесены в нее и в отношении которых не созданы правила оплаты.

Ближайшим аналогом заявленного способа является известный способ выполнения платежных транзакций, предусматривающий последовательное инициирование плательщиком запроса в платежную систему на транзакцию по передаче средств получателю, ввод плательщиком в платежную систему названия получателя и номинала платежа, сохранение в платежной системе деталей транзакции, в частности введенного плательщиком названия получателя, введенного плательщиком номинала платежа, а также условий выполнения транзакции, параметров аутентификации, создание получателем запроса в платежную систему на получение средств от плательщика, ввод в платежную систему получателем шаблонов аутентификации, проверку платежной системой введенных получателем шаблонов аутентификации, проверку условий выполнения транзакции, выполнение транзакции при успешной проверке либо отмене транзакции при неуспешной проверке [патент EP 2743873, МПК G 06Q 20/40, дата публикации 18.06.2014].

Особенностью известного способа является то, что условия выполнения транзакции и шаблоны аутентификации устанавливаются платежной системой и не могут быть установлены плательщиком. Способ не позволяет плательщику устанавливать для каждой вы-

полненной им транзакции индивидуальные условия выполнения этой транзакции и шаблоны аутентификации для получателя. Например, плательщик не может указать, что транзакция А может быть осуществлена только через три недели и при условии нахождения получателя Х в городе Париж, а транзакция В может быть выполнена только через пять дней и при условии нахождения получателя Y в городе Барселона.

Еще одним недостатком известного способа является невозможность установки плательщиком дополнительных шаблонов аутентификации. Например, плательщик не может указать, что транзакция А может быть осуществлена только при условии, если получатель Х введет в платежную систему определенный плательщиком именно для этой транзакции пин-код "97531" и введет в платежную систему фотографию почтовой открытки с изображением Пизанской башни.

Отсутствие возможности установить плательщиком определенные им условия выполнения транзакции и шаблоны аутентификации делают известный способ недостаточно надежным и негибким в использовании.

Кроме того, этот известный способ, как и преимущественное большинство других подобных способов, не позволяет выполнять транзакции в пользу получателя, название которого плательщику неизвестно, при этом гарантируя высокий уровень безопасности и надежности транзакции.

Ближайшим аналогом заявленной системы является известная система передачи средств, содержащая как минимум один процессинговый сервер, сервер сохранения шаблонов аутентификации [патент EP 2743873, МПК G 06Q 20/40, дата публикации 18.06.2014].

Недостатком известной системы является невозможность ввода и сохранения определенных плательщиком дополнительных условий аутентификации и определенных плательщиком дополнительных условий выполнения транзакции.

Задачей изобретения является создание способа и системы передачи цифровых ценностей, позволяющих плательщику при инициировании им запроса в систему на транзакцию по собственному желанию определять и вводить дополнительные условия осуществления транзакции (в частности, дату и время осуществления транзакции, желаемый период времени выполнения транзакции, данные о географическом месте расположения получателя), устанавливать и вводить дополнительные шаблоны аутентификации (пин-код, графическое изображение, аудиозапись, видеозапись, текст), надежно хранить информацию о выполненной транзакции с возможностью ее дальнейшего просмотра при необходимости.

В способе поставленная задача достигается в известном способе выполнения транзакции по передаче цифрового актива, при котором

направляют посредством коммуникационного устройства плательщика запрос транзакции на процессинговый сервер системы выполнения транзакций по передаче цифровых активов;

вводят в систему посредством коммуникационного устройства плательщика номинал передаваемого цифрового актива, имя и параметры аутентификации его получателя, тип, пин-код и основные условия выполнения транзакции и сохраняют указанные введенные данные на сервере сохранения шаблонов аутентификации указанной системы;

вводят в систему и сохраняют на сервере сохранения шаблонов аутентификации выбранные плательщиком дополнительные условия выполнения транзакции;

создают первичный ключ аутентификации в виде содержащего метаданные графического изображения заданного физического объекта либо серии таких изображений путем фотосъемки указанного объекта коммуникационным устройством плательщика и сохраняют указанный ключ на сервере сохранения шаблонов аутентификации;

сохраняют в публичном распределенном реестре информацию о запланированной транзакции, после чего блокируют в учетной записи плательщика передаваемый цифровой актив;

## BY 23492 C1 2021.08.30

информируют получателя о физическом объекте, использованном для создания первичного ключа аутентификации, и обо всех указанных, необходимых для выполнения транзакции;

направляют посредством коммуникационного устройства получателя запрос транзакции на процессинговый сервер;

вводят в систему посредством коммуникационного устройства получателя тип и пин-код транзакции, информацию о соблюдении указанных условий ее выполнения, а также первичный ключ аутентификации, воспроизведенный получателем с использованием того же физического объекта;

устанавливают подлинность всех введенных получателем данных путем их сравнения с теми же данными, ранее сохраненными плательщиком на сервере сохранения шаблонов аутентификации;

после чего списывают заблокированный актив с учетной записи плательщика, зачисляют его на учетную запись получателя, удаляют с сервера сохранения шаблонов аутентификации использованный первичный ключ аутентификации и сохраняют информацию о выполненной транзакции в публичном распределенном реестре.

В качестве дополнительных условий выполнения транзакции используют желаемую дату ее выполнения.

В качестве дополнительных условий выполнения транзакции используют данные о желаемом диапазоне дат ее выполнения.

В качестве дополнительных условий выполнения транзакции используют данные о географическом местоположении получателя.

После направления плательщиком запроса транзакции дополнительно создают вторичный ключ аутентификации, сохраняют его на сервере шаблонов и информируют о нем получателя, а после направления запроса получателем вводят в систему воспроизведенный получателем вторичный ключ аутентификации, после чего сравнивают его с тем же ключом, ранее сохраненным плательщиком на сервере сохранения шаблонов аутентификации.

В качестве вторичного ключа аутентификации используют содержащую метаданные аудиозапись.

В качестве вторичного ключа аутентификации используют содержащую метаданные видеозапись.

В качестве вторичного ключа аутентификации используют содержащий метаданные текстовый файл.

В качестве имени получателя вводят в систему указание на анонимного получателя.

Система выполнения транзакций по передаче цифровых активов указанным способом содержит взаимосвязанные

по меньшей мере один процессинговый сервер, выполненный с возможностью получения с коммуникационных устройств плательщика и получателя запросов транзакций, а также с возможностью списывания активов с учетной записи плательщика и их зачисления на учетную запись получателя;

сервер сохранения шаблонов аутентификации, выполненный с возможностью сохранения и удаления введенных в систему номиналов передаваемых цифровых активов, имени и параметров аутентификации получателя, типов, пин-кодов и условий выполнения транзакций, а также первичных ключей аутентификации, созданных в виде графических изображений заданного физического объекта, содержащих метаданные, либо серий таких изображений;

модуль проверки, выполненный с возможностью установления подлинности всех введенных получателем в систему данных транзакции путем их сравнения с теми же данными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации;

публичный распределенный реестр данных о транзакциях.

## BY 23492 C1 2021.08.30

Модуль проверки выполнен с возможностью сравнения аудиозаписей и их метаданных, введенных получателем, с такими же аудиозаписями и их метаданными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации.

Модуль проверки выполнен с возможностью сравнения видеозаписей и их метаданных, введенных получателем, с такими же видеозаписями и их метаданными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации.

Модуль проверки выполнен с возможностью сравнения текстовых файлов и их метаданных, введенных получателем, с такими же файлами и их метаданными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации.

Модуль проверки выполнен с возможностью сравнения желаемой даты осуществления транзакции, сохраненной плательщиком, с текущей датой транзакции.

Модуль проверки выполнен с возможностью сравнения данных о желаемом географическом местоположении получателя, сохраненных плательщиком, с данными о текущем местоположении получателя.

Реестр выполнен в виде сети взаимосвязанных аппаратно-программных комплексов.

Техническим результатом заявленного способа является повышение надежности выполнения транзакции за счет ввода в систему передачи цифровых активов определенных плательщиком дополнительных условий выполнения транзакции, пин-кода и первичных ключей аутентификации при инициировании плательщиком запроса в систему на транзакцию и дальнейшего ввода в систему получателем первичных ключей аутентификации.

В частности, безопасность выполнения транзакции повышается за счет того, что как первичный ключ аутентификации используют созданное плательщиком графическое изображение любого выбранного по желанию плательщика физического объекта и метаданные этого изображения. Соответственно, получателю, чтобы сформировать и ввести первичный ключ аутентификации, необходимо иметь в своем распоряжении тот самый физический предмет, который был у плательщика. Вместе с необходимостью ввода пин-кода такое решение исключает возможность получения цифрового актива мошенником, который попытается имитировать получателя.

Еще больше безопасность выполнения транзакции повышается за счет возможности указывать плательщиком вторичные ключи аутентификации, такие как: видеозапись с ее метаданными, аудиозапись с ее метаданными, текст с его метаданными.

Достигается возможность выполнения транзакции в определенную плательщиком дату и время или любой желаемый период времени (например, с отсрочкой на несколько дней, недель, месяцев) и в определенном плательщиком географическом месте расположения получателя. Это становится возможным за счет использования в качестве дополнительных условий выполнения транзакции указанных плательщиком даты, времени и периода времени выполнения транзакции, а также данных о географическом месте расположения получателя и дальнейшей проверки этих данных. При этом выполнение каждой транзакции, даже с отсрочкой на любое время, выполняется только в один шаг - путем списания предварительно заблокированного цифрового актива с учетной записи плательщика и его зачисления на учетную запись получателя. Это также позволяет повысить безопасность выполнения транзакции за счет отказа от использования промежуточных перезачислений на корреспондентские и транзитные счета, которые используются банковскими учреждениями и платежными системами.

Достигается возможность надежного сохранения информации о транзакции путем сохранения ее в публичном распределенном реестре. Поскольку публичный распределенный реестр сохраняется на неограниченном количестве соединенных между собой аппаратно-программных комплексов, исключается возможность подделки информации о транзакции.

Кроме того, становится возможным выполнение транзакций в пользу анонимного получателя (то есть получателя, название или имя которого неизвестны плательщику) с соблюдением высокого уровня безопасности и надежности транзакции за счет

## ВУ 23492 С1 2021.08.30

идентификации личности получателя только по первичным и/или вторичным ключам аутентификации.

Техническим результатом заявленной системы является предоставление плательщику возможности на свое усмотрение устанавливать и вводить в систему дополнительные условия выполнения транзакции и дополнительные шаблоны аутентификации получателя, что достигается за счет выполнения сервера сохранения шаблонов аутентификации с возможностью сохранения введенных плательщиком дополнительных условий выполнения транзакции, ключей аутентификации и пин-кода.

Также техническим результатом является возможность сравнивать ключи аутентификации, введенные плательщиком, с ключами аутентификации, введенными получателем, что, в свою очередь, становится возможным за счет включения в состав системы модуля проверки, способного сравнивать между собой графические изображения и их метаданные, аудиозаписи и их метаданные, видеозаписи и их метаданные, тексты и их метаданные. Это, в свою очередь, дает возможность выполнения транзакции даже когда название или имя получателя неизвестны плательщику (транзакции в пользу анонимного получателя).

Также техническим результатом является повышение надежности сохранения информации о транзакции путем выполнения публичного распределенного реестра, в котором она сохраняется в виде сети соединенных между собой аппаратно-программных комплексов. Поскольку публичный распределенный реестр сохраняется на неограниченном количестве соединенных между собой аппаратно-программных комплексов, исключается возможность подделки информации о транзакции. В случае повреждения или подделки реестра на одном аппаратно-программном комплексе она будет заменена неповрежденной копией с других аппаратно-программных комплексов.

Также техническим результатом является проверка соблюдения определенных плательщиком дополнительных условий выполнения транзакции, что становится возможным благодаря выполнению модуля проверки способным сравнивать данные о географическом месте расположения получателя, введенном плательщиком, с данными о текущем географическом месте расположения получателя, а также дате выполнения транзакции, введенной плательщиком, с текущей датой.

В приведенных ниже материалах будет подробно раскрыта суть заявленного способа выполнения транзакции по передаче цифровых активов и системы передачи цифровых активов для его осуществления.

В описании будет использована следующая терминология.

Цифровой актив - имущество и иные ценности, выраженный в виде буквенно-цифрового идентификатора и зарегистрированный в публичном распределенном реестре (блокчейн).

Метаданные - информация о другой информации или данных, касающихся дополнительной информации о содержании или объекте. Метаданные раскрывают сведения о признаках и свойствах, характеризующих любые сущности, которые позволяют автоматически искать и управлять ими в больших информационных потоках.

Bitbon - цифровой производный финансовый инструмент, имеющий идентификатор и номинал в объеме, определяемом в порядке, предусмотренном Публичным контрактом Bitbon, который соответствует определенной части имущественных прав на активы. Любые операции с Bitbon (выпуск, передача от одного владельца другому, дробление номинала и прочие операции) фиксируются в публичном распределенном реестре в виде записей, которые невозможно удалить или модифицировать.

Атрибутами Bitbon являются:

Идентификатор - уникальная последовательность буквенных и цифровых символов;

Номинал - число неограниченной глубины, соответствующее доле имущественных прав на активы пользователя;



Записи в публичном распределенном реестре, которые фиксируют все операции с каждым Bitbon;

Публичный контракт Bitbon.

Публичный контракт - цифровой актив, определяющий и регламентирующий область использования системы передачи цифровых активов, правила работы системы, шаблоны аутентификации пользователей.

Плательщик - пользователь системы, инициирующий транзакцию по передаче Цифрового актива, которым он владеет, другому пользователю.

Получатель - пользователь системы, получающий Цифровой актив от Плательщика.

Шаблоны аутентификации плательщика - определенная в соответствии с Публичным контрактом последовательность данных, идентифицирующая личность Плательщика.

Шаблоны аутентификации получателя - определенная в соответствии с Публичным контрактом последовательность данных, идентифицирующая личность Получателя.

Ключ аутентификации - последовательность цифровых данных, описывающих характеристики физического объекта, явления. Например, Ключом аутентификации могут быть цифровые данные, описывающие внешний вид почтовой открытки.

Первичный ключ аутентификации - созданное Плательщиком цифровое графическое изображение (либо серия изображений) любого физического объекта и Метаданные этого изображения (этих изображений). Примером Первичного ключа аутентификации могут быть цифровое графическое изображение почтовой открытки и Метаданные этого изображения.

Вторичный ключ аутентификации - введенная Плательщиком цифровая аудиозапись (видеозапись, текст) и Метаданные этой аудиозаписи (видеозаписи, текста).

Примером Вторичного ключа аутентификации могут быть цифровая аудиозапись автомобильного клаксона и Метаданные этой аудиозаписи.

Условия выполнения транзакции - определенные в соответствии с Публичным контрактом общие Условия выполнения транзакции в системе.

Дополнительные условия выполнения транзакции - определенные Плательщиком условия выполнения каждой определенной транзакции в системе, в частности дата выполнения транзакции, данные о желаемом периоде времени выполнения транзакции, данные о географическом месте расположения Получателя.

Заявленный способ и система иллюстрируются фигурами.

Фиг. 1 - состав системы передачи цифрового актива и взаимодействие ее компонентов.

Фиг. 2 - блок-схема реализации способа выполнения транзакции по передаче цифрового актива на примере электронных денег.

Фиг. 3 - блок-схема реализации способа выполнения транзакции по передаче цифрового актива на примере электронных денег (продолжение блок-схемы с фиг. 2).

Фиг. 4 - блок-схема реализации способа выполнения транзакции по передаче цифрового актива на примере электронных денег в пользу анонимного получателя.

Фиг. 5 - блок-схема реализации способа выполнения транзакции по передаче цифрового актива на примере электронных денег в пользу анонимного получателя (продолжение блок-схемы с фиг. 4).

Фиг. 6 - блок-схема реализации способа выполнения транзакции по передаче цифрового актива на примере Bitbon.

Фиг. 7 - блок-схема реализации способа выполнения транзакции по передаче цифрового актива на примере Bitbon (продолжение блок-схемы с фиг. 6).

Система выполнения транзакций по передаче цифровых активов содержит взаимосвязанные

по меньшей мере один процессинговый сервер 101, выполненный с возможностью получения с коммуникационных устройств плательщика и получателя запросов транзакций,

а также с возможностью списывания активов с учетной записи плательщика и их зачисления на учетную запись получателя;

сервер 102 сохранения шаблонов аутентификации, выполненный с возможностью сохранения и удаления введенных в систему номиналов передаваемых цифровых активов, имени и шаблонов аутентификации получателя, типов, пин-кодов и условий выполнения транзакций, а также первичных ключей аутентификации, созданных в виде графических изображений заданного физического объекта, содержащих метаданные, либо серий таких изображений;

модуль 103 проверки, выполненный с возможностью установления подлинности всех введенных получателем в систему данных транзакции путем их сравнения с теми же данными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации;

публичный распределенный реестр 104 данных о транзакциях.

Модуль 103 проверки выполнен также с возможностью сравнения аудиозаписей и их метаданных, введенных получателем, с такими же аудиозаписями и их метаданными, сохраненными плательщиком на сервере 102 сохранения шаблонов аутентификации.

Модуль 103 проверки может быть выполнен с возможностью сравнения видеозаписей и их метаданных, введенных получателем, с такими же видеозаписями и их метаданными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации.

Модуль 103 проверки выполнен также с возможностью сравнения текстовых файлов и их метаданных, введенных получателем, с такими же файлами и их метаданными, сохраненными плательщиком на сервере сохранения шаблонов аутентификации.

Модуль 103 проверки может быть выполнен с возможностью сравнения желаемой даты выполнения транзакции, сохраненной плательщиком, с текущей датой транзакции.

Модуль 103 проверки выполнен также с возможностью сравнения данных о желаемом географическом местоположении получателя, сохраненных плательщиком, с данными о текущем местоположении получателя.

Указанный реестр 104 выполнен в виде сети взаимосвязанных аппаратно-программных комплексов.

Плательщик взаимодействует с системой с помощью коммутатора 105.

Получатель взаимодействует с системой с помощью коммутатора 106.

Коммутаторами 105 и 106 могут быть программируемые устройства с возможностью соединения с Интернетом, в частности смартфоны, стационарные компьютеры, ноутбуки, планшеты и т.д.

Рассмотрим реализацию заявленного способа выполнения транзакции по передаче Цифрового актива и работу заявленной системы на примерах.

**Пример 1.** Способ выполнения транзакции по передаче Цифрового актива на примере электронных денег (фиг. 2, 3).

Осуществляют инициирование Плательщиком запроса на транзакцию по передаче Цифрового актива в виде определенной суммы электронных денег от Плательщика к Получателю (этап 210). При этом осуществляют аутентификацию Плательщика в системе в соответствии с Публичным контрактом (например, вводом логина и пароля). Запрос на транзакцию осуществляют с использованием коммуникационного устройства 105 Плательщика, который взаимодействует с системой с помощью современных средств связи. Вводят в систему название Получателя (например, John Smith) и номинал Цифрового актива - количество электронных денежных единиц (этап 220).

Вводят тип транзакции (например, приватная), пин-код (например, "12345"), Дополнительные условия выполнения транзакции, создают и вводят Первичный ключ аутентификации (этап 230). Например, Дополнительными условиями выполнения транзакции может быть введенная Плательщиком дата 01 сентября 2019 года, в которую Плательщик желает выполнить транзакцию по передаче Цифрового актива Получателю, а также название го-

рода Баден- Баден, в который Получатель должен прибыть для получения этой Цифрового актива.

Для создания Первичного ключа аутентификации Платательщик может использовать, например, почтовую открытку с фотографией Пизанской башни. Платательщик фотографирует эту открытку своим коммуникационным устройством 105. Программное обеспечение коммуникационного устройства 105 сохраняет изображение открытки в цифровом виде в формате графического файла, который, помимо данных об изображении, содержит Метаданные, касающиеся этого изображения. Первичным ключом аутентификации в этом случае будет созданное Платательщиком и сохраненное в цифровом виде графическое изображение почтовой открытки и Метаданные этого изображения.

Сохраняют на сервере 102 Первичный ключ аутентификации, пин-код, тип транзакции и Дополнительные условия выполнения транзакции (этап 240).

Сохраняют в публичном распределенном реестре 104 детали отложенной транзакции: название Получателя, номинал Цифрового актива, тип транзакции (этап 250).

Далее блокируют на учетной записи Плательщика Цифровой актив указанного Плательщиком номинала (этап 260).

После этого информируют Получателя о выполненной транзакции. Информирование может быть осуществлено системой в автоматическом режиме либо Плательщиком. Плательщик любым удобным способом в любое удобное время информирует Получателя о физическом объекте, использованном для создания Первичного ключа аутентификации, об указанных Дополнительных условиях выполнения транзакции, сообщает Получателю идентификатор транзакции и пин-код (этап 270).

Осуществляют запрос в процессинговые серверы 101 на получение Цифрового актива Получателем (этап 310). При этом осуществляют аутентификацию Получателя в системе в соответствии с Публичным контрактом (например, вводом логина и пароля). Запрос осуществляют с использованием коммуникационного устройства 106 Получателя.

Процессинговые серверы 101 валидируют запрос Получателя и, если его выполнение возможно, передают запрос на выдачу шаблонов аутентификации в модуль 103 проверки ключей, который, в свою очередь, отправляет запрос на сервер 102 сохранения шаблонов аутентификации. Сервер 102 отправляет Получателю на коммуникационное устройство 106 инструкции по созданию Первичного ключа аутентификации. В соответствии с полученными инструкциями Получатель должен ввести полученный от Плательщика пин-код "12345", сфотографировать полученную от Плательщика открытку с изображением Пизанской башни, сформировать с помощью программного обеспечения Метаданные этого изображения и, таким образом, воспроизвести Первичный ключ аутентификации. В модуль 103 проверки отправляют воспроизведенный Получателем Первичный ключ аутентификации (этап 320).

Сервер 102 отправляет введенный Плательщиком Первичный ключ аутентификации, который на нем сохранен, в модуль проверки 103. Также сервер 102 отправляет сохраненные на нем Дополнительные условия выполнения транзакции в модуль 103 проверки. Далее осуществляют проверку (этап 330) Первичного ключа аутентификации и Дополнительных условий выполнения транзакции в модуле 103 проверки. Проверку Первичного ключа аутентификации осуществляют путем сравнения графического изображения почтовой открытки и его Метаданных, введенных Плательщиком, с графическим изображением почтовой открытки и его Метаданными, введенными Получателем.

Также в модуле 103 проверки осуществляют проверку Дополнительных условий выполнения транзакции (этап 330). Для этого сравнивают дату 01 сентября 2019 года, введенную Плательщиком, с текущей датой, а также название города Баден-Баден, введенное Плательщиком, с данными о текущем географическом месте расположения Получателя.

Если Первичный ключ аутентификации либо хотя бы одно из Дополнительных условий выполнения транзакции не проходит проверку, то транзакцию отменяют (этап 340).

В случае успешной проверки Первичного ключа аутентификации и Дополнительных условий выполнения транзакции транзакция по передаче Цифрового актива от Плательщика к Получателю успешно выполняется (этап 350) путем осуществления процессинговым сервером 101 зачисления Цифрового актива с учетной записи Плательщика на учетную запись Получателя. Далее в публичном распределенном реестре 104 сохраняют запись о выполненной транзакции (этап 360).

На коммуникатор 105 Плательщика и коммуникатор 106 Получателя отправляют сообщение о завершении транзакции. Шаблоны ключей аутентификации на сервере 102 обозначают как изъятые и удаляют.

**Пример 2.** Способ выполнения транзакции по передаче Цифровых активов на примере электронных денег в пользу анонимного Получателя (фиг. 4, 5).

Осуществляют инициирование Плательщиком запроса на транзакцию по передаче Цифрового актива в виде определенной суммы электронных денег от Плательщика к анонимному Получателю (этап 410). При этом осуществляют аутентификацию Плательщика в системе в соответствии с Публичным контрактом (например, вводом логина и пароля). Запрос на транзакцию выполняют с использованием коммуникационного устройства 105 Плательщика, взаимодействующего с системой с помощью современных способов связи.

Вводят в систему указание на анонимного Получателя (например, Anonymous или John Doe) и номинал Цифрового актива - количество электронных денежных единиц (этап 420). Вводят тип транзакции (например, публичная), пин-код (например, "12345"), Дополнительные условия выполнения транзакции, создают и вводят Первичный ключ аутентификации (этап 430). Например, Дополнительными условиями выполнения транзакции может быть введенная Плательщиком дата 01 сентября 2019 года, в которую Плательщик желает выполнить транзакцию по передаче Цифрового актива Получателю, а также название города Мюнхен, в который Получатель должен прибыть для получения этого Цифрового актива.

Для создания Первичного ключа аутентификации Плательщик может использовать, например, наполовину полную стеклянную бутылку из-под Coca-Cola. Плательщик фотографирует бутылку своим коммуникационным устройством 105. Программное обеспечение коммуникационного устройства 105 сохраняет изображение бутылки в цифровом виде в формате графического файла, который, помимо данных об изображении, содержит Метаданные, касающиеся этого изображения. Первичным ключом аутентификации в этом случае будет созданное Плательщиком и сохраненное в цифровом виде графическое изображение бутылки из-под Coca-Cola и Метаданные этого изображения.

Для создания Вторичного ключа аутентификации Плательщик может использовать, например, песню Yellow Submarine группы The Beatles. Плательщик загружает эту песню в свое коммуникационное устройство 105. Программное обеспечение коммуникационного устройства 105 сохраняет песню в цифровом виде в формате аудиофайла, который, помимо данных о звуке, содержит Метаданные, касающиеся этого звука. Вторичным ключом аутентификации в этом случае будет цифровая аудиозапись и Метаданные этой аудиозаписи (этап 440).

Далее сохраняют на сервере 102 Первичный и Вторичный ключ аутентификации, пин-код, тип транзакции и Дополнительные условия выполнения транзакции (этап 450).

Сохраняют в публичном распределенном реестре 104 детали отложенной транзакции: указание на анонимного Получателя, номинал Цифрового актива, тип транзакции (этап 460).

Далее блокируют на учетной записи Плательщика Цифровой актив указанного Плательщиком номинала (этап 470).

После этого информируют Получателя о выполненной транзакции. Плательщик любым удобным способом в любое удобное время информирует Получателя о физическом объекте, использованном для создания Первичного ключа аутентификации, о песне, ис-

пользованной для создания Вторичного ключа аутентификации, об указанных им Дополнительных условиях выполнения транзакции, сообщает Получателю идентификатор транзакции и пин-код (этап 480). Например, Плательщик может осуществить информирование Получателя личным сообщением посредством электронной почты. Также возможно информирование неопределенного количества лиц путем размещения в публичном доступе информации о выполненной транзакции, Первичных и Вторичных ключах аутентификации и Дополнительных условиях выполнения транзакции. Такой способ информирования может быть полезным Плательщику для проведения масштабных рекламных акций и розыгрышей призов, когда заранее неизвестно, кто именно будет Получателем. Суть акции может быть, например, такой: Получателем транзакции станет тот человек из города Мюнхен, который первым 01 сентября 2019 года приобретет бутылку Coca-Cola и введет в систему указанные Плательщиком Первичные и Вторичные ключи аутентификации и пин-код.

Далее осуществляют запрос в процессинговые серверы 101 на получение Цифрового актива Получателем (этап 510). При этом осуществляют аутентификацию Получателя в системе в соответствии с Публичным контрактом (например, вводом логина и пароля). Запрос осуществляют с использованием коммуникационного устройства 106 Получателя.

Процессинговые серверы 101 валидируют запрос Получателя и, если его выполнение возможно, передают запрос на выдачу шаблонов аутентификации в модуль 103 проверки ключей, который, в свою очередь, отправляет запрос на сервер 102 сохранения шаблонов аутентификации. Сервер 102 отправляет Получателю на коммуникационное устройство 106 инструкции по созданию Первичного и Вторичного ключей аутентификации. В соответствии с полученными инструкциями Получатель должен ввести полученный от Плательщика пин-код "12345", сфотографировать наполовину полную бутылку из-под Coca-Cola, загрузить себе на коммуникационное устройство 106 песню Yellow Submarine группы The Beatles, сформировать с помощью программного обеспечения Метаданные изображения и аудиозаписи и, таким образом, воспроизвести Первичный и Вторичный ключи аутентификации. В модуль 103 проверки передают воспроизведенный Получателем Первичный ключ аутентификации (этап 520) и воспроизведенный Получателем Вторичный ключ аутентификации (этап 530).

Сервер 102 отправляет введенные Плательщиком Первичный и Вторичный ключи аутентификации, сохраненные на нем, в модуль проверки 103. Также сервер 102 отправляет сохраненные на нем Дополнительные условия выполнения транзакции в модуль 103 проверки. Далее осуществляют проверку (этап 540) Первичного и Вторичного ключей аутентификации и Дополнительных условий выполнения транзакции в модуле 103 проверки. Проверку Первичного ключа аутентификации осуществляют путем сравнения графического изображения бутылки и его Метаданных, введенных Плательщиком, с графическим изображением бутылки и его Метаданными, введенными Получателем. Проверку Вторичного ключа аутентификации осуществляют путем сравнения аудиозаписи и ее Метаданных, введенных Плательщиком, с аудиозаписью и ее Метаданными, введенными Получателем.

Также в модуле 103 проверки осуществляют проверку Дополнительных условий выполнения транзакции (этап 540). Для этого сравнивают дату 01 сентября 2019 года, введенную Плательщиком, с текущей датой, а также название города Мюнхен, введенное Плательщиком, с данными о текущем географическом месте расположения Получателя.

Если Первичный ключ аутентификации или Вторичный ключ аутентификации или хотя бы одно из Дополнительных условий выполнения транзакции не проходит проверку, то транзакцию отменяют (этап 550).

При успешной проверке Первичного и Вторичного ключей аутентификации, а также всех Дополнительных условий выполнения транзакции эта транзакция по передаче Цифрового актива от Плательщика к анонимному Получателю успешно выполняется (этап

560) путем осуществления процессинговым сервером 101 зачисления Цифрового актива с учетной записи Плательщика на учетную запись Получателя. Далее в публичном распределенном реестре 104 сохраняют запись о выполненной транзакции (этап 570).

На коммуникатор 105 Плательщика и коммуникатор 106 Получателя отправляют сообщение о завершении транзакции. Шаблоны ключей аутентификации на сервере 102 обозначают как изъятые и удаляют.

**Пример 3.** Способ выполнения транзакции по передаче Цифровой актива на примере Bitbon (фиг. 6, 7).

Перед передачей Цифрового актива в виде Bitbon осуществляют процедуру выпуска Bitbon. Подробно эта процедура описана заявителем в заявке на изобретение № а201701536, которая подана в Укрпатент 20.02.2017.

Осуществляют инициирование Плательщиком (владельцем Bitbon) запроса на транзакцию по передаче Цифрового актива в виде Bitbon от Плательщика к Получателю в соответствии с Публичным контрактом Bitbon (этап 610). Запрос на транзакцию выполняют с использованием коммуникационного устройства 105 Плательщика, которое взаимодействует с системой с помощью современных средств связи.

Вводят в систему название Получателя (например, John Smith) и номинал Цифрового актива - количество Bitbon (этап 620).

Вводят тип транзакции (например, приватная), пин-код (например, "12345"), Дополнительные условия выполнения транзакции, создают и вводят Первичный ключ аутентификации (этап 630). Например, Дополнительными условиями выполнения транзакции может быть введенная Плательщиком дата 01 сентября 2019 года, в которую Плательщик желает выполнить транзакцию по передаче Bitbon Получателю, а также название города Лондон, в который Получатель должен прибыть для получения Bitbon.

Для создания Первичного ключа аутентификации Плательщик может использовать, например, статуэтку в виде кота. Плательщик фотографирует статуэтку кота своим коммуникационным устройством 105. Программное обеспечение коммуникационного устройства 105 сохраняет изображение статуэтки в цифровом виде в формате графического файла, который, помимо данных об изображении, содержит Метаданные, касающиеся этого изображения. Первичным ключом аутентификации в этом случае будет созданное Плательщиком и сохраненное в цифровом виде графическое изображение статуэтки и Метаданные этого изображения.

Далее сохраняют на сервере 102 Первичный ключ аутентификации, пин-код, тип транзакции и Дополнительные условия выполнения транзакции (этап 640).

Сохраняют в публичном распределенном реестре 104 детали отложенной транзакции: название Получателя, номинал Bitbon, тип транзакции (этап 650).

Далее блокируют на учетной записи Плательщика Bitbon указанного Плательщиком номинала (этап 660).

После этого информируют Получателя о выполненной транзакции. Информирование может быть осуществлено системой в автоматическом режиме либо Плательщиком. Плательщик любым удобным способом в любое удобное время информирует Получателя о физическом объекте, использованном для создания Первичного ключа аутентификации, об указанных Дополнительных условиях выполнения транзакции, передает Получателю идентификатор транзакции и пин-код (этап 670).

Осуществляют запрос в процессинговые серверы 101 на получение Цифрового актива Получателем (этап 710). При этом осуществляют аутентификацию Получателя в системе в соответствии с Публичным контрактом (например, вводом логина и пароля). Запрос осуществляют с использованием коммуникационного устройства 106 Получателя. Процессинговые серверы 101 валидируют запрос Получателя и, если его выполнение возможно, передают запрос на выдачу шаблонов аутентификации в модуль 103 проверки ключей,

который, в свою очередь, отправляет запрос на сервер 102 сохранения шаблонов аутентификации.

Сервер 102 отправляет Получателю на коммуникационное устройство 106 инструкции по созданию Первичного ключа аутентификации. В соответствии с полученными инструкциями Получатель должен ввести полученный от Плательщика пин-код "12345", сфотографировать полученную от Плательщика статуэтку кота, сформировать с помощью программного обеспечения Метаданные этого изображения и, таким образом, воспроизвести Первичный ключ аутентификации. Воспроизведенный Получателем Первичный ключ аутентификации отправляют в модуль 103 проверки (этап 720).

Сервер 102 отправляет введенный Плательщиком Первичный ключ аутентификации, сохраненный на нем, в модуль 103 проверки. Также сервер 102 отправляет сохраненные на нем Дополнительные условия осуществления транзакции в модуль 103 проверки. Далее осуществляют проверку (этап 730) Первичного ключа аутентификации и Дополнительных условий выполнения транзакции в модуле 103 проверки. Проверку Первичного ключа аутентификации осуществляют путем сравнения графического изображения статуэтки кота и его Метаданных, введенных Плательщиком, с графическим изображением статуэтки кота и его Метаданными, введенными Получателем.

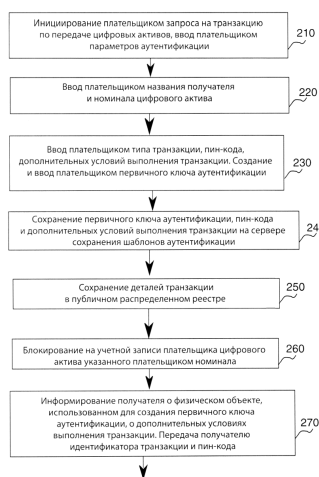
Также в модуле 103 проверки осуществляют проверку Дополнительных условий выполнения транзакции (этап 730). Для этого сравнивают дату 01 сентября 2019 года, введенную Плательщиком, с текущей датой, а также название города Лондон, введенное Плательщиком, с данными о текущем географическом месте расположения Получателя.

Если Первичный ключ аутентификации или хотя бы одно из Дополнительных условий выполнения транзакции не проходит проверку, то транзакцию отменяют (этап 740).

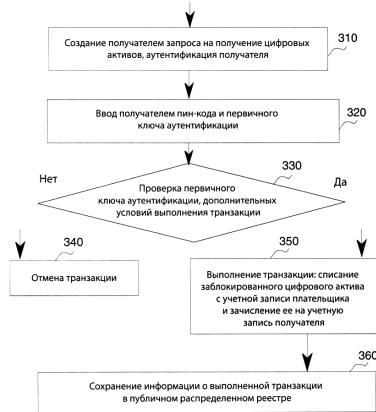
В случае успешной проверки Первичного ключа аутентификации и Дополнительных условий выполнения транзакции указанная транзакция по передаче Bitbon от Плательщика к Получателю успешно выполняется (этап 750) путем осуществления процессинговым сервером 101 зачисления Bitbon с учетной записи Плательщика на учетную запись Получателя. Далее в публичном распределенном реестре 104 сохраняют запись о выполненной транзакции (этап 760).

На коммуникатор 105 Плательщика и коммуникатор 106 Получателя отправляют сообщение о завершении транзакции. Шаблоны Артефактов аутентификации на сервере 102 обозначают как изъятые и удаляют.

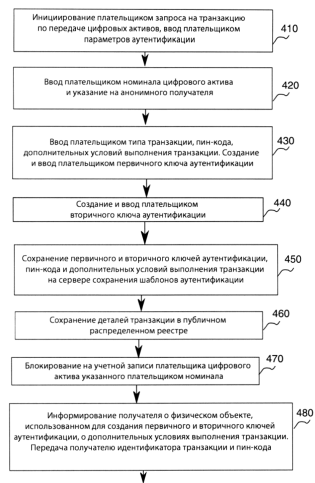
Приведенные выше примеры использования заявленного способа и системы только иллюстрируют возможности их осуществления и ни в коем случае не ограничивают сферу использования заявленного способа и системы.



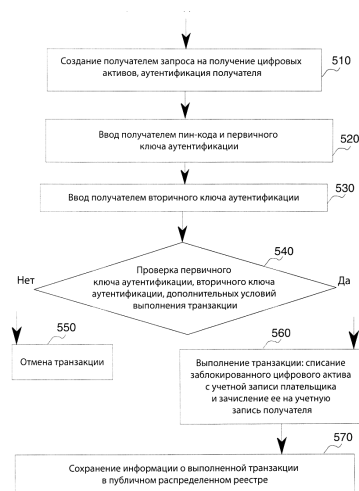
Фиг. 2



Фиг. 3

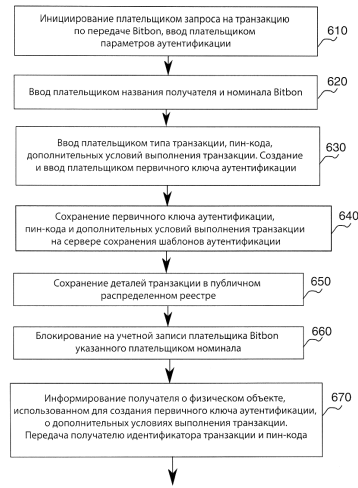


Фиг. 4

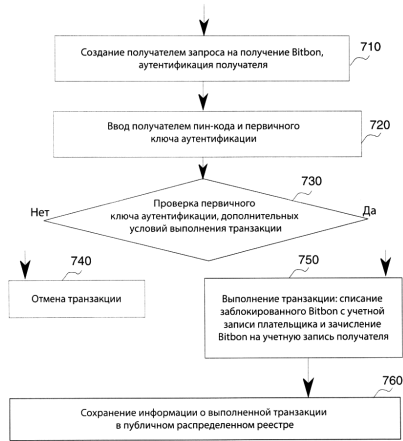


Фиг. 5





Фиг. 6



Фиг. 7