(19) Евразийское патентное ведомство

(21) 201891901 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2019.03.29

(22) Дата подачи заявки
2016.03.29

(51) Int. Cl. ***G06F 17/30*** (2006.01)
G06Q 20/36 (2012.01)
G06Q 20/38 (2012.01)

(54) СИСТЕМА И СПОСОБ ДЛЯ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ЛИЧНОСТИ НА ОСНОВЕ БЛОКЧЕЙНА

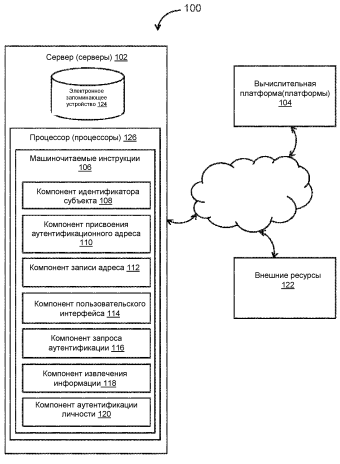
(31) **15/083,241**
(32) **2016.03.28**
(33) **US**
(86) **PCT/US2016/024776**
(87) **WO 2017/171733 2017.10.05**

(71) Заявитель:
БЛЭК ГОЛД КОЙН, ИНК. (US)

(72) Изобретатель:
Андраде Маркус (US)

(74) Представитель:
Угрюмов В.М., Гизатуллина Е.М., Строкова О.В., Глухарёва А.О. (RU)

(57) Может быть обеспечена многофакторная аутентификация личности на основе блокчейна. Аутентификационные адреса в блокчейне можно создавать путем установления соответствия идентификаторов субъектам, чья личность была ранее аутентифицирована, присвоения аутентификационных адресов в блокчейне указанным субъектам и записи идентификаторов и биометрических данных, связанных с субъектами, по соответствующим аутентификационным адресам. Многофакторную аутентификацию личности на основе блокчейна с помощью аутентификационных адресов можно выполнять путем получения одного или более идентификаторов в связи с одним или более запросами аутентификации личности одного или более субъектов, извлечения биометрических данных, связанных с указанными одним или более субъектами, из соответствующих аутентификационных адресов и аутентификации личности одного или более субъектов при получении совпадающих биометрических данных и секретных ключей.



201891901 A1

201891901 A1

СИСТЕМА И СПОСОБ ДЛЯ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ЛИЧНОСТИ НА ОСНОВЕ БЛОКЧЕЙНА

Область техники, к которой относится изобретение

(01) Настоящее раскрытие относится к системам и способам для обеспечения многофакторной аутентификации личности на основе блокчейна.

Раскрытие изобретения

(02) В одном аспекте раскрытие относится к системе для обеспечения многофакторной аутентификации личности на основе блокчейна. Система может содержать один или более аппаратных процессоров, выполненных с машиночитаемыми инструкциями для создания аутентификационных адресов в блокчейне и/или выполнения многофакторной аутентификации личности на основе блокчейна с помощью указанных аутентификационных адресов. Создание аутентификационных адресов в блокчейне может включать в себя установление соответствия идентификаторов субъектам, чьи личности ранее были аутентифицированы, при этом устанавливают соответствие первого идентификатора первому субъекту, при этом личность первого субъекта ранее была аутентифицирована; присвоение аутентификационных адресов в блокчейне указанным субъектам, при этом отдельно взятый аутентификационный адрес включает в себя открытый ключ и секретный ключ, при этом первый аутентификационный адрес присваивают первому субъекту, при этом первый аутентификационный адрес включает в себя первый открытый ключ и первый секретный ключ; и записывание идентификаторов и биометрических данных, связанных с указанными субъектами, по соответствующим аутентификационным адресам, при этом первый идентификатор и первые биометрические данные, связанные с первым субъектом, записывают по первому аутентификационному адресу. Выполнение многофакторной аутентификации личности на основе блокчейна с помощью аутентификационных адресов может включать в себя получение одного или более идентификаторов в связи с одним или более запросами аутентификации личности одного или более субъектов, при этом первый идентификатор получают в связи с запросом аутентификации личности первого субъекта; извлечение биометрических данных, связанных с одним или

более субъектами, из соответствующих аутентификационных адресов, при этом первые биометрические данные, связанные с первым субъектом, извлекают из первого аутентификационного адреса; и аутентификацию личности одного или более субъектов при получении совпадающих биометрических данных и секретных ключей, при этом личность первого субъекта аутентифицируют при получении (1) биометрических данных, совпадающих с первыми биометрическими данными, и (2) секретного ключа, совпадающего с первым секретным ключом.

(03) В другом аспекте раскрытие относится к способу для создания аутентификационных адресов в блокчейне для обеспечения многофакторной аутентификации личности на основе блокчейна. Способ можно выполнять посредством одного или более аппаратных процессоров, выполненных с машиночитаемыми инструкциями. Способ может содержать этапы, на которых: устанавливают соответствие идентификаторов субъектам, чьи личности ранее были аутентифицированы, при этом устанавливают соответствие первого идентификатора первому субъекту, при этом личность первого субъекта ранее была аутентифицирована; присваивают аутентификационные адреса в блокчейне указанным субъектам, при этом отдельно взятый аутентификационный адрес включает в себя открытый ключ и секретный ключ, при этом первый аутентификационный адрес присваивают первому субъекту, при этом первый аутентификационный адрес включает в себя первый открытый ключ и первый секретный ключ; и записывают идентификаторы и биометрические данные, связанные с указанными субъектами, по соответствующим аутентификационным адресам, при этом первый идентификатор и первые биометрические данные, связанные с первым субъектом, записывают по первому аутентификационному адресу. Личность одного или более субъектов может быть аутентифицирована при получении совпадающих биометрических данных и секретных ключей, при этом личность первого субъекта аутентифицируют при получении (1) биометрических данных, совпадающих с первыми биометрическими данными, и (2) секретного ключа, совпадающего с первым секретным ключом.

(04) В еще одном аспекте раскрытие относится к способу для выполнения многофакторной аутентификации личности на основе блокчейна с помощью аутентификационных адресов. Способ можно выполнять посредством одного или более аппаратных процессоров, выполненных с машиночитаемыми

инструкциями. Способ может содержать этапы, на которых: получают один или более идентификаторов в связи с одним или более запросами аутентификации личности одного или более субъектов, при этом первый идентификатор получают в связи с запросом аутентификации личности первого субъекта; извлекают биометрические данные, связанные с одним или более субъектами, из соответствующих аутентификационных адресов в блокчейне, при этом отдельно взятый аутентификационный адрес включает в себя открытый ключ и секретный ключ, при этом первые биометрические данные, связанные с первым субъектом, извлекают из первого аутентификационного адреса, присвоенного первому субъекту, при этом первый аутентификационный адрес включает в себя первый открытый ключ и первый секретный ключ; и аутентифицируют личность одного или более субъектов при получении совпадающих биометрических данных и секретных ключей, при этом личность первого субъекта аутентифицируют при получении (1) биометрических данных, совпадающих с первыми биометрическими данными, и (2) секретного ключа, совпадающего с первым секретным ключом.

(05) Указанные и прочие признаки и характеристики предлагаемой технологии, способы эксплуатации и функции относящихся к ней элементов конструкции и комбинации деталей, а также экономические показатели изготовления, станут более понятны после рассмотрения нижеследующего раздела «Осуществление изобретения» и прилагаемой формулы изобретения, раскрытых на примере прилагаемых чертежей, все из которых являются частью настоящего описания, причем аналогичные номера позиций обозначают соответствующие детали на разных фигурах. При этом следует понимать, что чертежи служат исключительно для цели иллюстрирования и описания, а не предназначены для определения границ изобретения. В тексте описания и формулы изобретения формы единственного числа «один», «некоторый» и «указанный» включают в себя ссылки к формам множественного числа, если иное явно не следует из контекста.

Краткое описание чертежей

(06) ФИГ.1 иллюстрирует систему для обеспечения многофакторной аутентификации личности на основе блокчейна по одному или более вариантам осуществления.

(07) ФИГ.2 иллюстрирует способ для создания аутентификационных адресов в блокчейне для обеспечения многофакторной аутентификации личности на основе блокчейна по одному или более вариантам осуществления.

(08) ФИГ.3 иллюстрирует способ для выполнения многофакторной аутентификации личности на основе блокчейна с помощью аутентификационных адресов по одному или более вариантам осуществления.

Осуществление изобретения

(09) ФИГ.1 иллюстрирует систему 100 для обеспечения многофакторной аутентификации личности на основе блокчейна по одному или более вариантам осуществления. В некоторых вариантах система 100 может содержать один или более серверов 102. Сервер (серверы) 102 может быть выполнен с возможностью осуществления связи с одной или более вычислительными платформами 104 в соответствии с клиент-серверной архитектурой, одноранговой архитектурой и/или иными архитектурами. Пользователи могут осуществлять доступ к системе 100 посредством вычислительной платформы (платформ) 104.

(10) Сервер (серверы) 102 может быть выполнен с возможностью исполнения машиночитаемых инструкций 106. Машиночитаемые инструкции 106 могут включать в себя: компонент 108 идентификатора субъекта, и/или компонент 110 присвоения аутентификационного адреса, и/или компонент 112 записи адреса, и/или компонент 114 пользовательского интерфейса, и/или компонент 116 запроса аутентификации, и/или компонент 118 извлечения информации, и/или компонент 120 аутентификации личности, и/или иные компоненты машиночитаемых инструкций.

(11) Машиночитаемые инструкции 106 можно исполнять для создания аутентификационных адресов в блокчейне. По существу, блокчейн представляет собой базу данных транзакций, коллективно используемую некоторыми или всеми узлами, принимающими участие в системе 100. Их участие может происходить на основе протокола Биткойн (англ. Bitcoin), протокола Эфириум (англ. Ethereum) и/или иных протоколов, относящихся к цифровым валютам и/или блокчейнам. Полная версия блокчейна включает в себя каждую когда-либо выполненную транзакцию в соответствующей цифровой валюте. В дополнение к

транзакциям, блокчейн может содержать и другую информацию, как будет подробнее раскрыто в настоящем описании.

(12) В основе блокчейна могут лежать несколько блоков. Блок может содержать запись, содержащую или подтверждающую одну или более ожидающих транзакций. Периодически (например, приблизительно раз в минуту) может происходить прибавление нового блока, содержащего транзакции и/или иную информацию, к блокчейну. В некоторых вариантах отдельно взятый блок в блокчейне содержит хеш предыдущего блока. Результатом этого может стать создание цепочки блоков от первичного блока (т.е. первого блока в блокчейне) до текущего блока. Данный отдельно взятый блок может гарантированно хронологически следовать за предыдущим блоком, так как в противном случае хеш предыдущего блока не был бы известен. Модификация данного отдельно взятого блока после его включения в блокчейн может быть практична с вычислительной точки зрения, так как для этого нужна была бы регенерация каждого блока после него.

(13) Данный отдельно взятый аутентификационный адрес может включать в себя конкретное место в блокчейне, где происходит хранение некой информации. В некоторых вариантах индивидуальный аутентификационный адрес может именоваться «адрес AtenVerify». Аутентификационные адреса подробнее раскрыты ниже на примере компонента 110 присвоения аутентификационного адреса.

(14) Компонент 108 идентификатора субъекта может быть выполнен с возможностью установления соответствия идентификаторов субъектам, чья личность была ранее аутентифицирована. Например, может быть установлено соответствие первого идентификатора первому субъекту. Личность первого субъекта может быть ранее аутентифицирована. По существу, идентификатор может включать в себя число, буквенно-цифровой код, имя пользователя и/или иную информацию, которая может быть связана с субъектом. В некоторых вариантах индивидуальный идентификатор может именоваться «Aten ID».

(15) По некоторым вариантам осуществления, аутентификация личности субъекта, чья личность была ранее аутентифицирована, могла быть получена несколькими путями. Например, в некоторых вариантах индивида могут запросить предоставить свидетельство, удостоверяющее его личность.

Предоставление такого свидетельства может включать в себя предоставление экземпляра выданного государственным органом идентификационного документа (например, паспорта и/или водительских прав), предоставление экземпляра почтовой корреспонденции, полученной субъектом (например, счета за коммунальные услуги), свидетельства третьего лица и/или иного свидетельства, удостоверяющего личность субъекта. Указанное свидетельство может быть предоставлено организации, связанной с сервером (серверами) 102.

(16) Компонент 110 присвоения аутентификационного адреса может быть выполнен с возможностью присвоения субъектам аутентификационных адресов в блокчейне. Отдельно взятый аутентификационный адрес может включать в себя открытый ключ и секретный ключ. Например, первый аутентификационный адрес может быть присвоен первому субъекту. Первый аутентификационный адрес может включать в себя первый открытый ключ и первый секретный ключ.

(17) В общем, пару «открытый и секретный ключ» можно использовать для шифрования и дешифрования по одному или нескольким алгоритмам с открытым ключом. В качестве неограничивающего примера, пару ключей можно применять для цифровых подписей. Такая пара ключей может содержать секретный ключ для подписания и открытый ключ для аутентификации. Открытый ключ можно широко распространять, при этом секретный ключ держат в тайне (например, он известен только его владельцу). Указанные ключи могут быть связаны друг с другом математически, при этом вычисление секретного ключа из открытого ключа невыполнимо.

(18) В некоторых вариантах осуществления компонент 110 присвоения аутентификационного адреса может быть выполнен с возможностью хранения секретных ключей в пределах вычислительной платформы (платформ) 104. Например, первый секретный ключ можно хранить в пределах вычислительной платформы 104 и/или других мест, относящихся к первому субъекту. По некоторым вариантам секретный ключ можно хранить в файле “verify.dat”, и/или на SIM-карте, и/или в других местах.

(19) В некоторых вариантах осуществления компонент 110 присвоения аутентификационного адреса может быть выполнен с возможностью присвоения нескольких аутентификационных адресов отдельным субъектам. Например, в дополнение к первому аутентификационному адресу первому субъекту может

быть присвоен второй аутентификационный адрес. Первому субъекту можно присвоить один или более дополнительных аутентификационных адресов, в соответствии с одним или более вариантами осуществления.

(20) Компонент 112 записи адреса может быть выполнен с возможностью записи идентификаторов и биометрических данных, связанных с субъектами, по соответствующим аутентификационным адресам. Например, первый идентификатор и первые биометрические данные, связанные с первым субъектом, могут быть записаны по первому аутентификационному адресу. Запись информации по отдельно взятому аутентификационному адресу может включать в себя запись хеша или иного зашифрованного представления информации. В некоторых вариантах разные биометрические данные можно записывать по нескольким аутентификационным адресам, присвоенным одному и тому же субъекту. Например, в дополнение к первому идентификатору и первым биометрическим данным, связанным с первым субъектом, записываемым по первому аутентификационному адресу, по второму аутентификационному адресу могут быть записаны первый идентификатор и вторые биометрические данные, связанные с первым субъектом.

(21) В общем, биометрические данные могут включать в себя метрические показатели, относящиеся к характеристикам человека. Биометрические идентификаторы представляют собой отличительные измеримые характеристики, могущие служить для обозначения и описания субъектов. Биометрические идентификаторы обычно включают в себя физиологические характеристики, однако могут также включать в себя поведенческие характеристики и/или иные характеристики. Физиологические характеристики могут относиться к форме тела субъекта. В число примеров физиологических характеристик, служащих в качестве биометрических данных, могут входить одна или более из следующих: отпечаток пальца, вены ладони, распознавание лица, ДНК, отпечаток ладони, геометрия кисти руки, распознавание по радужной оболочке глаза, сетчатка глаза, запах и/или иные физиологические характеристики. Поведенческие характеристики могут быть связаны с характером поведения субъекта. В число примеров поведенческих характеристик, служащих в качестве биометрических данных, могут входить одна или более из следующих: клавиатурный почерк, походка, голос и/или иные поведенческие характеристики.

(22) Биометрические данные могут включать в себя: изображение или иное

визуальное представление физиологической характеристики, и/или запись поведенческой характеристики, и/или шаблон физиологической характеристики и/или поведенческой характеристики, и/или иные биометрические данные. Шаблон может включать в себя обобщение существенных признаков, извлеченных из источника. Шаблон может включать в себя вектор, описывающий признаки физиологической характеристики и/или поведенческой характеристики, и/или числовое представление физиологической характеристики и/или поведенческой характеристики, и/или изображение с конкретными свойствами, и/или иную информацию.

(23) Биометрические данные можно получить посредством вычислительных платформ 104, связанных с субъектами. Например, биометрические данные, связанные с первым субъектом, можно получить посредством первой вычислительной платформы 104, связанной с первым субъектом. Первая вычислительная платформа 104 может содержать устройство ввода (не показано), выполненное с возможностью фиксации и/или записи физиологической характеристики и/или поведенческой характеристики первого субъекта. В число примеров такого устройства ввода могут входить одно или более из следующих: съемочная камера и/или иной формирователь изображений, сканер отпечатков пальцев, микрофон, акселерометр и/или иные устройства ввода.

(24) Компонент 114 пользовательского интерфейса может быть выполнен с возможностью создания интерфейса для представления субъектам посредством соответствующих вычислительных платформ 104. Интерфейс может включать в себя графический пользовательский интерфейс, представленный посредством индивидуальных вычислительных платформ 104. По некоторым вариантам осуществления интерфейс может быть выполнен с возможностью добавления или удаления отдельно взятым субъектом аутентификационных адресов, присвоенных данному отдельно взятому субъекту, при условии, что данному отдельно взятому субъекту присвоен по меньшей мере один аутентификационный адрес.

(25) В некоторых вариантах осуществления компонент 114 пользовательского интерфейса может быть выполнен с возможностью доступа к одному или более профилям пользователей и/или информации о пользователе, относящимся к пользователям системы 100, и/или управления ими. Один или более профилей

пользователей и/или информация о пользователе может содержать информацию, хранимую на сервере (серверах) 102, одной или более из вычислительных платформ 104 и/или в иных местах хранения. Профили пользователей могут содержать, например, информацию, идентифицирующую пользователей (например, имя или псевдоним пользователя, номер, идентификатор и/или иную идентифицирующую информацию), данные для безопасного входа в систему (например, код или пароль для входа в систему), данные учетной записи в системе, информацию о подписке, данные о счете в цифровой валюте (например, относящиеся к валюте, находящейся в кредитовой части счета пользователя), информацию о связи (например, информацию о связях между пользователями в системе 100), информацию об использовании системы, демографическую информацию, относящуюся к пользователям, статистику взаимодействия между пользователями в системе 100, информацию, указанную пользователями, информацию о покупках пользователей, статистику просмотра пользователями, идентификационные данные вычислительной платформы, связанные с пользователем, номер телефона, связанный с пользователем, и/или иную информацию, относящуюся к пользователям.

(26) Машиночитаемые инструкции 106 можно исполнять для выполнения многофакторной аутентификации личности на основе блокчейна с помощью указанных аутентификационных адресов.

(27) Компонент 116 запроса аутентификации может быть выполнен с возможностью получения одного или более идентификаторов в связи с одним или более запросами аутентификации личности одного или более субъектов. Например, первый идентификатор может быть получен в связи с запросом аутентификации личности первого субъекта. Запросы аутентификации личности могут быть выданы в связи с финансовыми транзакциями, обменами информацией и/или иными взаимодействиями и/или относиться к ним. Запросы могут быть получены от других субъектов и/или третьих лиц.

(28) Компонент 118 извлечения информации может быть выполнен с возможностью извлечения биометрических данных, связанных с одним или более субъектами, из соответствующих аутентификационных адресов. Например, первые биометрические данные, связанные с первым субъектом, можно извлечь из первого аутентификационного адреса. Извлечение информации (например, биометрических данных) с аутентификационного адреса может включать в себя

дешифрование информации.

(29) По некоторым вариантам осуществления компонент 118 извлечения информации может быть выполнен с возможностью, в качестве реакции на получение запроса аутентификации личности первого субъекта, выдачи первому субъекту запроса на ввод биометрических данных, совпадающих с первыми биометрическими данными, и секретного ключа, совпадающего с первым секретным ключом. Запрос на ввод может быть передан посредством вычислительной платформы 104, соответствующей первому субъекту. Запрос на ввод может быть передан посредством графического пользовательского интерфейса и/или иного пользовательского интерфейса, образованного вычислительной платформой 104, соответствующей первому субъекту. Запрос на ввод может содержать указание, представляющее собой визуальное, и/или звуковое, и/или осязательное и/или иные указания.

(30) В некоторых вариантах осуществления компонент 118 извлечения информации может быть выполнен с возможностью, в качестве реакции на получение запроса аутентификации личности первого субъекта, выдачи запроса на ввод вычислительной платформе 104, связанной с первым субъектом. В ответ на запрос на ввод вычислительная платформа 104 может автоматически выдать серверу (серверам) 102 биометрические данные, совпадающие с первыми биометрическими данными, и/или секретный ключ, совпадающий с первым секретным ключом.

(31) Компонент 120 аутентификации личности может быть выполнен с возможностью аутентификации личности одного или более субъектов при получении или в качестве реакции на получение совпадающих биометрических данных и секретных ключей. Например, личность первого субъекта можно аутентифицировать при получении (1) биометрических данных, совпадающих с первыми биометрическими данными, и (2) секретного ключа, совпадающего с первым секретным ключом. Выполнение аутентификации личности первого субъекта может включать в себя сравнение сохраненной информации с только что полученной информацией.

(32) По некоторым вариантам осуществления компонент 120 аутентификации личности может быть выполнен с возможностью аутентификации личности первого субъекта при получении (1) биометрических данных, совпадающих с

первыми биометрическими данными, или вторых биометрических данных и (2) секретного ключа, совпадающего с первым секретным ключом. Такие варианты осуществления могут предусматривать так называемые «подписи M-из-N» для аутентификации личности, для которой нужно некое подмножество более крупного множества идентификационной информации.

(33) В некоторых вариантах осуществления компонент 120 аутентификации личности может быть выполнен с возможностью применения биометрических данных, совпадающих с первыми биометрическими данными, и секретного ключа, совпадающего с первым секретным ключом, для подписания аутентификации личности первого субъекта.

(34) Криптографическая подпись представляет собой математический механизм, обеспечивающий возможность подтверждения принадлежности чего-либо кому-либо. В случае Биткойна, кошелек в системе «Биткойн» и его секретный ключ (ключи) связаны между собой некой математической магической схемой. Когда программное обеспечение системы «Биткойн» подписывает транзакцию посредством соответствующего секретного ключа, вся сеть может видеть то, что подпись соответствует тратимым биткойнам. При этом никто не может разгадать секретный ключ для похищения ваших заработанных тяжелым трудом биткойнов.

(35) В некоторых вариантах осуществления подписание аутентификации личности первого субъекта выполняет по меньшей мере один специальный узел. Отдельно взятый специальный узел может включать в себя один или более серверов 102. Данный отдельно взятый специальный узел может представлять собой узел общего пользования или частный узел, выполненный с возможностью создания новых блоков и/или подписания аутентификации.

(36) В некоторых вариантах сервер (серверы) 102, вычислительная платформа (платформы) 104, и/или внешние ресурсы 122 могут быть функционально связаны посредством одного или более каналов электронной связи. Например, такие каналы электронной связи могут быть созданы, по меньшей мере частично, посредством сети, например – сети интернет и/или иных сетей. Следует понимать, что данный пример не является ограничивающим, и в объем настоящего раскрытия входят варианты осуществления, в которых сервер (серверы) 102, вычислительная платформа (платформы) 104 и/или внешние

ресурсы 122 могут быть функционально связаны посредством какого-либо другого средства связи.

(37) Отдельно взятая вычислительная платформа 104 может содержать один или более процессоров, выполненных с возможностью исполнения машиночитаемых инструкций. Машиночитаемые инструкции могут обеспечивать возможность взаимодействия специалиста или пользователя, связанного с данной отдельно взятой вычислительной платформой 104, с системой 100 и/или внешними ресурсами 122, и/или выполнения иных функций, относимых в настоящем описании к вычислительной платформе (платформам) 104. В качестве неограничивающего примера, данная отдельно взятая вычислительная платформа 104 может включать в себя: настольный компьютер, портативный компьютер, карманный компьютер, планшетный компьютер, нетбук, смартфон, игровую приставку и/или иные вычислительные платформы.

(38) В число внешних ресурсов 122 могут входить источники информации, главные вычислительные узлы и/или поставщики виртуальных сред за пределами системы 100, сторонние организации, участвующие в системе 100, и/или иные ресурсы. В некоторых вариантах некоторые или все функции, относимые в настоящем описании к внешним ресурсам 100, могут выполнять ресурсы, содержащиеся в системе 100.

(39) Сервер (серверы) 102 может включать в себя электронное запоминающее устройство 124, один или более процессоров 126 и/или иные компоненты. Сервер (серверы) 102 может включать в себя каналы или порты связи для обеспечения возможности обмена информацией с какой-либо сетью и/или другими вычислительными платформами. Иллюстрация сервера (серверов) 102 на ФИГ.1 не носит ограничивающего характера. Сервер (серверы) 102 может включать в себя множество аппаратных, программных и/или программно-аппаратных компонентов, работающих совместно для выполнения функций, в настоящем описании относимых к серверу (серверам) 102. Например, сервер (серверы) 102 может быть реализован посредством облачной среды вычислительных платформ, работающих совместно в качестве сервера (серверов) 102.

(40) Электронное запоминающее устройство 124 может включать в себя долговременный носитель данных, хранящий информацию в электронной форме. Электронный носитель данных электронного запоминающего устройства

124 может представлять собой системное запоминающее устройство, выполненное за одно целое (т.е. по существу без возможности снятия) с сервером (серверами) 102, и/или съемное запоминающее устройство, соединенное с возможностью снятия с сервером (серверами) 102 посредством, например, разъема (например, разъема универсальной последовательной шины USB, разъема шины «firewire» и т.п.), или накопитель (например, накопитель на дисках и т.п.). Электронное запоминающее устройство 124 может включать в себя оптический носитель данных (например, оптические диски и т.п.), и/или магнитный носитель данных (например, магнитную ленту, накопитель на жестких магнитных дисках, накопитель на гибких дисках и т.п.), и/или электрически-стираемый носитель данных (например, ЭСППЗУ, ОЗУ и т.п.), и/или твердотельный носитель данных (например, флеш-накопитель и т.п.), и/или иной электронно-читаемый носитель данных. Электронное запоминающее устройство 124 может включать в себя один или более виртуальных ресурсов хранения (например, облачное хранилище, виртуальную частную сеть и/или иные виртуальные ресурсы хранения). Электронное запоминающее устройство 124 выполнено с возможностью хранения программно-реализованных алгоритмов, информации, определенной процессором (процессорами) 126, информации, полученной от сервера (серверов) 102, информации, полученной от вычислительной платформы (платформ) 104, и/или иной информации, обеспечивающей возможность функционирования сервера (серверов) 102, как раскрыто в настоящем описании.

(41) Процессор (процессоры) 126 может быть выполнен для обеспечения возможностей обработки информации в сервере (серверах) 102. По существу, процессор (процессоры) 126 может включать в себя цифровой процессор, и/или аналоговый процессор, и/или цифровую схему, предназначенную для обработки информации, и/или аналоговую схему, предназначенную для обработки информации, и/или конечный автомат, и/или иные механизмы для электронной обработки информации. Несмотря на то, что процессор (процессоры) 126 показан на ФИГ.1 как единичный объект, это сделано исключительно в иллюстративных целях. В некоторых вариантах процессор (процессоры) 126 может включать в себя множество процессорных устройств. Данные процессорные устройства могут быть физически расположены в пределах одного и того же устройства, либо процессор (процессоры) 126 может представлять собой функции обработки,

выполняемые множеством согласованно работающих устройств. Процессор (процессоры) 126 может быть выполнен с возможностью реализации компонентов 108, 110, 112, 114, 116, 118, 120 машиночитаемых инструкций и/или иных компонентов машиночитаемых инструкций. Процессор (процессоры) 126 может быть выполнен с возможностью реализации компонентов 108, 110, 112, 114, 116, 118, 120 машиночитаемых инструкций и/или иных компонентов машиночитаемых инструкций посредством программных механизмов; аппаратных механизмов; программно-аппаратных механизмов; программных, аппаратных и/или программно-аппаратных механизмов в какой-либо комбинации; и/или иных механизмов для создания возможностей обработки в процессоре (процессорах) 126. В контексте настоящего описания термин «компонент машиночитаемой инструкции» может означать любой компонент или набор компонентов, выполняющий функции, относимые к компоненту машиночитаемой инструкции. Он может включать в себя физические процессоры во время исполнения читаемых процессором инструкций, читаемые процессором инструкции, электрические схемы, аппаратное обеспечение, носители данных или любые другие компоненты.

(42) Следует понимать, что, несмотря на то, что компоненты 108, 110, 112, 114, 116, 118 и 120 машиночитаемых инструкций проиллюстрированы на ФИГ.1 как реализованные в пределах одного и того же процессорного устройства, в вариантах осуществления, в которых процессор (процессоры) 126 включает в себя несколько процессорных устройств, один или более компонентов 108, 110, 112, 114, 116, 118 и/или 120 машиночитаемых инструкций могут быть реализованы удаленно от других компонентов машиночитаемых инструкций. Представленное ниже описание функций, выполняемых различными компонентами 108, 110, 112, 114, 116, 118 и/или 120 машиночитаемых инструкций носит иллюстративный, а не ограничивающий, характер, поскольку число функций, выполняемых любым из компонентов 108, 110, 112, 114, 116, 118 и/или 120 машиночитаемых инструкций, может быть больше или меньше, чем раскрыто. Например, один или более компонентов 108, 110, 112, 114, 116, 118 и/или 120 машиночитаемых инструкций можно исключить, при этом некоторые или все его функции могут выполнять другие компоненты 108, 110, 112, 114, 116, 118 и/или 120 машиночитаемых инструкций. В качестве другого примера, процессор (процессоры) 126 могут быть выполнены с возможностью реализации

одного или более дополнительных компонентов машиночитаемых инструкций, могущих выполнять некоторые или все функции, которые ниже отнесены к одному из компонентов 108, 110, 112, 114, 116, 118 и/или 120 машиночитаемых инструкций.

(43) ФИГ.2 иллюстрирует способ 200 для создания аутентификационных адресов в блокчейне для обеспечения многофакторной аутентификации личности на основе блокчейна по одному или более вариантам осуществления. Раскрытые ниже этапы способа 200 носят иллюстративный характер. В некоторых вариантах способ 200 можно осуществлять с одним или более дополнительными этапами, которые не раскрыты, и/или без одного или более из раскрытых этапов. Кроме того, порядок, в котором этапы способа 200 проиллюстрированы на ФИГ.2 и раскрыты ниже, не носит ограничивающего характера.

(44) В некоторых вариантах один или более этапов способа 200 можно осуществлять в одном или более процессорных устройствах (например, цифровом процессоре, аналоговом процессоре, цифровой схеме, предназначенной для обработки информации, аналоговой схеме, предназначенной для обработки информации, конечном автомате и/или иных механизмах для электронной обработки информации). В число одного или более процессорных устройств могут входить одно или более устройств, исполняющих некоторые или все из этапов способа 200 в соответствии с инструкциями, хранящимися в электронном виде на электронном носителе данных. Одно или более процессорных устройств могут включать в себя одно или более устройств, выполненных посредством аппаратных, программно-аппаратных и/или программных средств специально для исполнения одного или более этапов способа 200.

(45) На этапе 202 может быть установлено соответствие идентификаторов субъектам, чья личность была ранее аутентифицирована. Может быть установлено соответствие первого идентификатора первому субъекту. Личность первого субъекта может быть аутентифицирована ранее. Этап 202 можно выполнять посредством одного или более аппаратных процессоров, выполненных с возможностью реализации компонента машиночитаемой инструкции, идентичного или аналогичного компоненту 108 идентификатора субъекта (раскрытому на примере ФИГ.1) по одному или более вариантам

осуществления.

(46) На этапе 204 субъектам можно присвоить аутентификационные адреса в блокчейне. Отдельно взятый аутентификационный адрес может содержать открытый ключ и секретный ключ. Первый аутентификационный адрес можно присвоить первому субъекту. Первый аутентификационный адрес может содержать первый открытый ключ и первый секретный ключ. Этап 204 можно выполнять посредством одного или более аппаратных процессоров, выполненных с возможностью реализации компонента машиночитаемой инструкции, идентичного или аналогичного компоненту 110 присвоения аутентификационного адреса (раскрытому на примере ФИГ.1) по одному или более вариантам осуществления.

(47) На этапе 206 идентификаторы и биометрические данные, связанные с субъектами, можно записать по соответствующим аутентификационным адресам. Первый идентификатор и первые биометрические данные, связанные с первым субъектом, можно записать по первому аутентификационному адресу. Личность одного или более субъектов может быть аутентифицирована при получении или в качестве реакции на получение совпадающих биометрических данных и секретных ключей. Личность первого субъекта может быть аутентифицирована при получении или в качестве реакции на получение (1) биометрических данных, совпадающих с первыми биометрическими данными, и (2) секретного ключа, совпадающего с первым секретным ключом. Этап 206 можно выполнять посредством одного или более аппаратных процессоров, выполненных с возможностью реализации компонента машиночитаемой инструкции, идентичного или аналогичного компоненту 112 записи адреса (раскрытому на примере ФИГ.1) по одному или более вариантам осуществления.

(48) ФИГ.3 иллюстрирует способ 300 для выполнения многофакторной аутентификации личности на основе блокчейна с помощью аутентификационных адресов по одному или более вариантам осуществления. Раскрытые ниже этапы способа 300 носят иллюстративный характер. В некоторых вариантах способ 300 можно осуществлять с одним или более дополнительными этапами, которые не раскрыты, и/или без одного или более из раскрытых этапов. Кроме того, порядок, в котором этапы способа 300 проиллюстрированы на ФИГ.3 и раскрыты ниже, не носит ограничивающего характера.

(49) В некоторых вариантах осуществления способ 300 можно выполнять в одном или более процессорных устройствах (например, цифровом процессоре, аналоговом процессоре, цифровой схеме, предназначенной для обработки информации, аналоговой схеме, предназначенной для обработки информации, конечном автомате и/или иных механизмах для электронной обработки информации). В число одного или более процессорных устройств могут входить одно или более устройств, исполняющих некоторые или все из этапов способа 300 в соответствии с инструкциями, хранящимися в электронном виде на электронном носителе данных. Одно или более процессорных устройств могут включать в себя одно или более устройств, выполненных посредством аппаратных, программно-аппаратных и/или программных средств специально для исполнения одного или более этапов способа 300.

(50) На этапе 302 можно получить один или более идентификаторов в связи с одним или более запросами аутентификации личности одного или более субъектов. Первый идентификатор может быть получен в связи с запросом аутентификации личности первого субъекта. Этап 302 можно выполнять посредством одного или более аппаратных процессоров, выполненных с возможностью реализации компонента машиночитаемой инструкции, идентичного или аналогичного компоненту 116 запроса аутентификации (раскрытому на примере ФИГ.1) по одному или более вариантам осуществления.

(51) На этапе 304 можно извлечь биометрические данные, связанные с одним или более субъектами, из соответствующих аутентификационных адресов в блокчейне. Отдельно взятый аутентификационный адрес может содержать открытый ключ и секретный ключ. Первые биометрические данные, связанные с первым субъектом, можно извлечь из первого аутентификационного адреса, присвоенного первому субъекту. Первый аутентификационный адрес может содержать первый открытый ключ и первый секретный ключ. Этап 304 можно выполнять посредством одного или более аппаратных процессоров, выполненных с возможностью реализации компонента машиночитаемой инструкции, идентичного или аналогичного компоненту 118 извлечения информации (раскрытому на примере ФИГ.1) по одному или более вариантам осуществления.

(52) На этапе 306 можно аутентифицировать личность одного или более субъектов при получении или в качестве реакции на получение совпадающих

биометрических данных и секретных ключей. Личность первого субъекта можно аутентифицировать при получении или в качестве реакции на получение (1) биометрических данных, совпадающих с первыми биометрическими данными, и (2) секретного ключа, совпадающего с первым секретным ключом. Этап 306 можно выполнять посредством одного или более аппаратных процессоров, выполненных с возможностью реализации компонента машиночитаемой инструкции, идентичного или аналогичного компоненту 120 аутентификации личности (раскрытому на примере ФИГ.1) по одному или более вариантам осуществления.

(53) Примеры вариантов осуществления могут облегчить сохранение персональных данных в блокчейне. Персональные данные можно хранить в блокчейне в зашифрованном виде. Лицо можно идентифицировать на уровне блокчейна по секретному ключу, и/или отпечатку пальца, и/или хешу отпечатка пальца, и/или сетчатке глаза, и/или хешу сетчатки глаза, и/или иной уникальной информации. Сохраненные данные могут включать в себя паспорт, удостоверение личности, избранную информацию из паспорта, водительское удостоверение, избранную информацию из водительского удостоверения, отпечаток пальца, сетчатку глаза и/или иную информацию или относиться к ним. По некоторым вариантам осуществления, если некоторые данные будут изменены, для данного лица может быть создана новая запись в блокчейне. То есть все изменения вносят в виде новых записей. Старую запись всегда сохраняют в блокчейне. По существу, все записи в блокчейне хранят вечно и без возможности удаления. Будут существовать более одного экземпляра блокчейна во избежание манипуляций с записями.

(54) Примеры вариантов осуществления могут облегчить доступ к персональным данным. Могут существовать несколько уровней доступа для персональных данных в блокчейне. Ограничения доступа могут быть установлены на уровнях пар «открытый ключ и секретный ключ». В число примеров уровней доступа могут входить один или более из следующих: «Супер Администратор» (полный доступ к блокчейну), «Органы власти» - на уровне страны (полный доступ только для чтения), «Органы власти» - на уровне штата/местном уровне (ограниченный доступ только для чтения), «Полиция и иные службы, в том числе – аварийно-спасательные» (доступ к некоторым персональным данным только по отпечатку пальца/сетчатке глаза лица),

«Участвующие торговцы» (ограниченный доступ) и/или иные уровни доступа.

(55) Примеры вариантов осуществления могут облегчить проверку аутентификации. Могут существовать несколько уровней возможности проверки аутентификации. Например, некоторые варианты осуществления могут обеспечивать возможность наличия у лица записи в «Компании» без предоставления персональных данных. Некоторые варианты осуществления могут обеспечивать возможность наличия у лица записи в Компании и получения по существу базовых персональных данных, например – полного имени, даты рождения, пола и/или иных базовых данных. Некоторые варианты осуществления могут обеспечивать возможность наличия у лица записи в Компании и получения всех персональных данных.

(56) Несмотря на то, что предложенная технология была подробно раскрыта в иллюстративных целях на примерах вариантов осуществления, в настоящее время считающихся имеющими наибольшее практическое значение и наиболее предпочтительными, следует понимать, что указанное подробное раскрытие осуществлено исключительно с этой целью и то, что указанная технология не ограничена раскрытыми вариантами осуществления, а напротив включает в себя модификации и эквивалентные варианты, не отступающие от сущности и объема прилагаемой формулы изобретения. Например, следует понимать, что предложенная технология предусматривает то, что, по мере возможности, один или более признаков любого из вариантов осуществления можно комбинировать с одним или более признаками любого другого варианта осуществления.

ФОРМУЛА ИЗОБРЕТЕНИЯ:

1. Система для обеспечения многофакторной аутентификации личности на основе блокчейна, при этом система содержит:

один или более аппаратных процессоров, выполненных с машиночитаемыми инструкциями для:

создания аутентификационных адресов в блокчейне путем:

установления соответствия идентификаторов субъектам, чьи личности ранее были аутентифицированы, при этом устанавливают соответствие первого идентификатора первому субъекту, при этом личность первого субъекта ранее была аутентифицирована;

присвоения аутентификационных адресов в блокчейне субъектам, при этом отдельно взятый аутентификационный адрес включает в себя открытый ключ и секретный ключ, при этом первый аутентификационный адрес присваивают первому субъекту, при этом первый аутентификационный адрес включает в себя первый открытый ключ и первый секретный ключ; и

записи идентификаторов и биометрических данных, связанных с субъектами, по соответствующим аутентификационным адресам, при этом первый идентификатор и первые биометрические данные, связанные с первым субъектом, записывают по первому аутентификационному адресу; и

выполнения многофакторной аутентификации личности на основе блокчейна с помощью указанных аутентификационных адресов путем:

получения одного или более идентификаторов в связи с одним или более запросами аутентификации личности одного или более субъектов, при этом первый идентификатор получают в связи с запросом аутентификации личности первого субъекта;

извлечения биометрических данных, связанных с одним или более субъектами, из соответствующих аутентификационных адресов, при этом первые биометрические данные, связанные с первым субъектом,

извлекают из первого аутентификационного адреса; и

аутентификации личности одного или более субъектов при получении совпадающих биометрических данных и секретных ключей, при этом личность первого субъекта аутентифицируют при получении (1) биометрических данных, совпадающих с первыми биометрическими данными, и (2) секретного ключа, совпадающего с первым секретным ключом.

2. Система по п. 1, в которой первый секретный ключ сохранен в пределах вычислительной платформы, связанной с первым субъектом.

3. Система по п. 1, в которой предусмотрена возможность присваивания нескольких аутентификационных адресов отдельным субъектам так, чтобы первому субъекту был присвоен второй аутентификационного адреса в дополнение к первому аутентификационному адресу.

4. Система по п. 1, в которой указанные один или более аппаратных процессоров также выполнены с машиночитаемыми инструкциями для создания интерфейса для представления субъектам посредством соответствующих вычислительных платформ, при этом интерфейс выполнен с возможностью добавления или удаления отдельно взятым субъектом аутентификационных адресов, присвоенных данному отдельно взятому субъекту, при условии, что данному отдельно взятому субъекту присвоен по меньшей мере один аутентификационный адрес.

5. Система по п. 1, в которой предусмотрена возможность записи разных биометрических данных по нескольким аутентификационным адресам, присвоенным отдельно взятому субъекту, так, чтобы, в дополнение к первому идентификатору и первым биометрическим данным, связанным с первым субъектом, записываемым по первому аутентификационному адресу, первый идентификатор и вторые биометрические данные, связанные с первым субъектом, были записаны по второму аутентификационному адресу.

6. Система по п. 5, в которой предусмотрена возможность аутентификации личности первого субъекта при получении (1) биометрических данных, совпадающих с первыми биометрическими данными, или вторых биометрических данных и (2) секретного ключа, совпадающего с первым секретным ключом.

7. Система по п. 1, в которой биометрические данные включают в себя изображение, и/или запись, и/или шаблон.

8. Система по п. 1, в которой биометрические данные относятся к отпечатку пальца, и/или венам ладони, и/или распознаванию лица, и/или ДНК, и/или отпечатку ладони, и/или геометрии кисти руки, и/или распознаванию по радужной оболочке глаза, и/или сетчатке глаза, и/или запаху, и/или клавиатурному почерку, и/или походке, и/или голосу.

9. Система по п. 1, в которой первые биометрические данные получают посредством вычислительной платформы, связанной с первым субъектом.

10. Система по п. 1, в которой указанные один или более аппаратных процессоров также выполнены с машиночитаемыми инструкциями для выдачи запроса на ввод первым субъектом биометрических данных, совпадающих с первыми биометрическими данными, и секретного ключа, совпадающего с первым секретным ключом, в качестве реакции на получение запроса аутентификации личности первого субъекта, при этом запрос на ввод передают посредством вычислительной платформы, связанной с первым субъектом.

11. Система по п. 1, в которой указанные один или более аппаратных процессоров также выполнены с машиночитаемыми инструкциями для выдачи запроса на ввод вычислительной платформе, связанной с первым субъектом, для автоматического предоставления биометрических данных, совпадающих с первыми биометрическими данными, и секретного ключа, совпадающего с первым секретным ключом, в качестве реакции на получение запроса аутентификации личности первого субъекта.

12. Система по п. 1, в которой предусмотрена возможность использования

биометрических данных, совпадающих с первыми биометрическими данными, и секретного ключа, совпадающего с первым секретным ключом, для подписания аутентификации личности первого субъекта.

13. Система по п. 1, в которой предусмотрена возможность подписания аутентификации личности первого субъекта, выполняемой по меньшей мере одним специальным узлом.

14. Способ для создания аутентификационных адресов в блокчейне для обеспечения многофакторной аутентификации личности на основе блокчейна, при этом способ выполняют посредством одного или более аппаратных процессоров, выполненных с машиночитаемыми инструкциями, при этом способ содержит этапы, на которых:

устанавливают соответствие идентификаторов субъектам, чьи личности ранее были аутентифицированы, при этом устанавливают соответствие первого идентификатора первому субъекту, при этом личность первого субъекта ранее была аутентифицирована;

присваивают аутентификационные адреса в блокчейне указанным субъектам, при этом отдельно взятый аутентификационный адрес включает в себя открытый ключ и секретный ключ, при этом первый аутентификационный адрес присваивают первому субъекту, при этом первый аутентификационный адрес включает в себя первый открытый ключ и первый секретный ключ; и

записывают идентификаторы и биометрические данные, связанные с указанными субъектами, по соответствующим аутентификационным адресам, при этом первый идентификатор и первые биометрические данные, связанные с первым субъектом, записывают по первому аутентификационному адресу;

причем личность одного или более субъектов можно аутентифицировать при получении совпадающих биометрических данных и секретных ключей, при этом личность первого субъекта можно аутентифицировать при получении (1) биометрических данных, совпадающих с первыми биометрическими данными, и (2) секретного ключа, совпадающего с первым секретным ключом.

15. Способ по п. 14, в котором дополнительно присваивают несколько аутентификационных адресов отдельным субъектам так, чтобы, в дополнение к

первому аутентификационному адресу, первому субъекту был присвоен второй аутентификационный адрес.

16. Способ по п. 14, в котором дополнительно создают интерфейс для представления субъектам посредством соответствующих вычислительных платформ, при этом интерфейс выполнен с возможностью добавления или удаления отдельно взятым субъектом аутентификационных адресов, присвоенных данному отдельно взятому субъекту, при условии, что данному отдельно взятому субъекту присвоен по меньшей мере один аутентификационный адрес.

17. Способ по п. 14, в котором дополнительно записывают разные биометрические данные по нескольким аутентификационным адресам, присвоенным отдельно взятому субъекту, так, чтобы, в дополнение к первому идентификатору и первым биометрическим данным, связанным с первым субъектом, записываемым по первому аутентификационному адресу, первый идентификатор и вторые биометрические данные, связанные с первым субъектом были записаны по второму аутентификационному адресу.

18. Способ для выполнения многофакторной аутентификации личности на основе блокчейна с помощью аутентификационных адресов, при этом способ выполняют посредством одного или более аппаратных процессоров, выполненных с машиночитаемыми инструкциями, при этом способ содержит этапы, на которых:

получают один или более идентификаторов в связи с одним или более запросами аутентификации личности одного или более субъектов, при этом первый идентификатор получают в связи с запросом аутентификации личности первого субъекта;

извлекают биометрические данные, связанные с одним или более субъектами, из соответствующих аутентификационных адресов в блокчейне, при этом отдельно взятый аутентификационный адрес включает в себя открытый ключ и секретный ключ, при этом первые биометрические данные, связанные с первым субъектом, извлекают из первого аутентификационного адреса, присвоенного первому субъекту, при этом первый аутентификационный адрес

включает в себя первый открытый ключ и первый секретный ключ; и

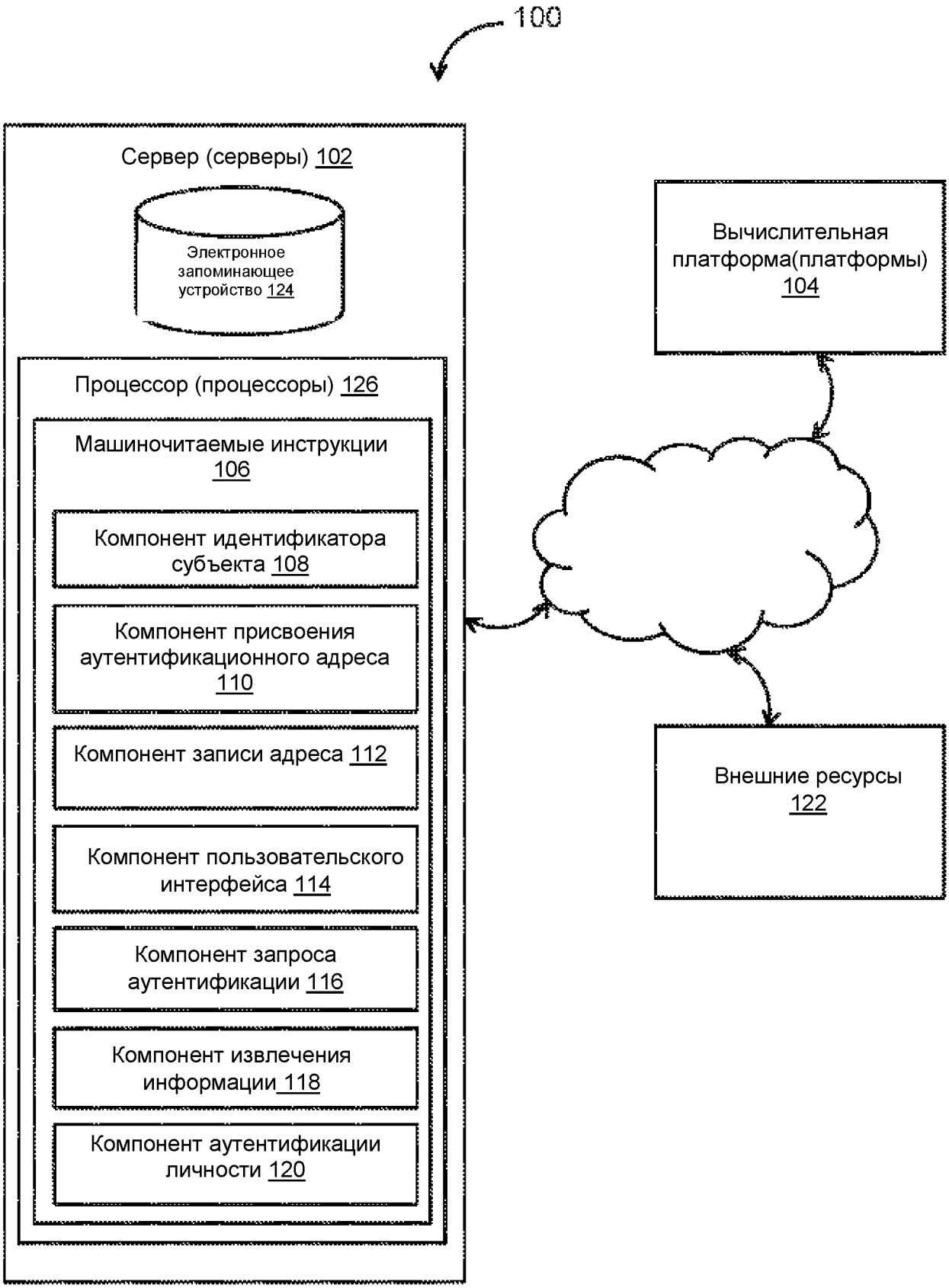
аутентифицируют личность одного или более субъектов при получении совпадающих биометрических данных и секретных ключей, при этом личность первого субъекта аутентифицируют при получении (1) биометрических данных, совпадающих с первыми биометрическими данными, и (2) секретного ключа, совпадающего с первым секретным ключом.

19. Способ по п. 18, в котором дополнительно, в качестве реакции на получение запроса аутентификации личности первого субъекта:

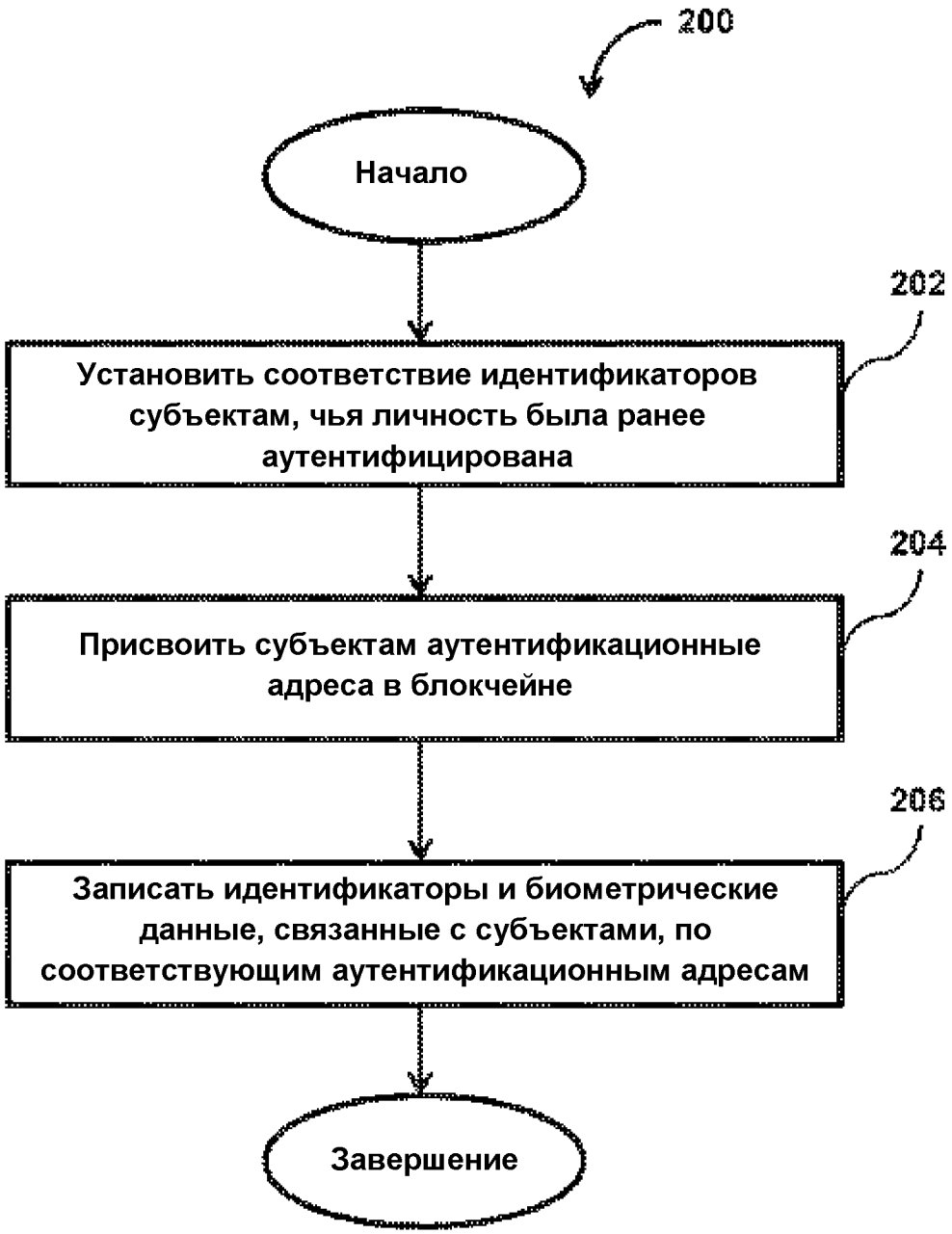
выдают первому субъекту запрос на ввод биометрических данных, совпадающих с первыми биометрическими данными, и секретного ключа, совпадающего с первым секретным ключом, при этом запрос на ввод передают посредством вычислительной платформы, связанной с первым субъектом; или

выдают вычислительной платформе, связанной с первым субъектом, запрос на ввод для автоматического предоставления биометрических данных, совпадающих с первыми биометрическими данными, и секретного ключа, совпадающего с первым секретным ключом.

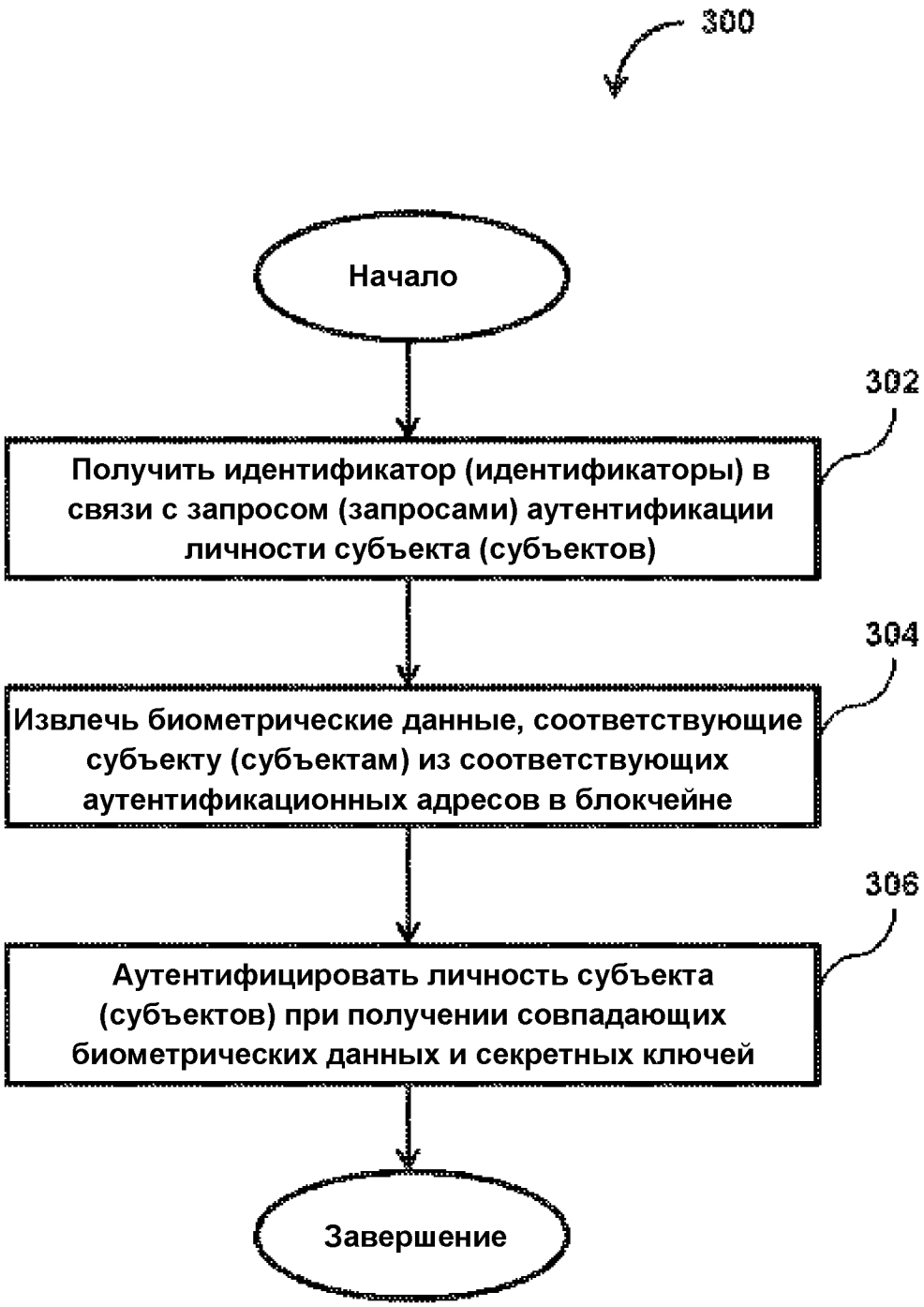
20. Способ по п. 18, в котором биометрические данные, совпадающие с первыми биометрическими данными, и секретный ключ, совпадающий с первым секретным ключом, применяют для подписания аутентификации личности первого субъекта.


100
Сервер (серверы) 102
Электронное запоминающее устройство 124
Процессор (процессоры) 126
Машиночитаемые инструкции 106
Компонент идентификатора субъекта 108
Компонент присвоения аутентификационного адреса 110
Компонент записи адреса 112
Компонент пользовательского интерфейса 114
Компонент запроса аутентификации 116
Компонент извлечения информации 118
Компонент аутентификации личности 120
Вычислительная платформа(платформы) 104
Внешние ресурсы 122

ФИГ. 1


200
Начало
202
Установить соответствие идентификаторов субъектам, чья личность была ранее аутентифицирована
204
Присвоить субъектам аутентификационные адреса в блокчейне
206
Записать идентификаторы и биометрические данные, связанные с субъектами, по соответствующим аутентификационным адресам
Завершение

ФИГ.2


300
Начало
302
Получить идентификатор (идентификаторы) в связи с запросом (запросами) аутентификации личности субъекта (субъектов)
304
Извлечь биометрические данные, соответствующие субъекту (субъектам) из соответствующих аутентификационных адресов в блокчейне
306
Аутентифицировать личность субъекта (субъектов) при получении совпадающих биометрических данных и секретных ключей
Завершение

ФИГ.3