(19) Евразийское патентное ведомство

(11) 040877 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.08.10

(21) Номер заявки
202190845

(22) Дата подачи заявки
2019.11.15

(51) Int. Cl. ***H04L 9/32*** (2006.01)

(54) НЕЙРОННЫЙ БЛОКЧЕЙН

(31) **102018000010379**
(32) **2018.11.16**
(33) **IT**
(43) **2021.08.05**
(86) **PCT/EP2019/081468**
(87) **WO 2020/099629 2020.05.22**

(71)(73) Заявитель и патентовладелец:
ЭЙБИСИДИ ТЕКНОЛОДЖИ САРЛ (CH)

(72) Изобретатель:
Бенвенути Джакомо (FR)

(74) Представитель:
Нилова М.И. (RU)

(56) JOHNG HAAN ET AL.: "Using Blockchain to Enhance the Trustworthiness of Business Processes: A Goal-Oriented Approach", 2018 IEEE INTERNATIONAL CONFERENCE ON SERVICES COMPUTING (SCC), IEEE, 2 July 2018 (2018-07-02), pages 249-252, XP033399025, DOI: 10.1109/SCC.2018.00041 abstract Chapter II. "Fides: a Framework for BPR using Blockchain"; page 249, right-hand column - page 252, left-hand column
CN-A-107508680
US-A1-2018103042
US-A1-2017230375
US-A1-2018268401

(57) Изобретение относится к реализуемой с помощью компьютера системе для безопасных хранения и передачи цифровых данных между пользователями на основании протокола наподобие блокчейн и к реализуемому с помощью компьютера способу, использующему указанную компьютерную систему.

040877 B1

040877 B1

Область техники

Изобретение относится к реализуемой с помощью компьютера системе и реализуемому с помощью компьютера способу безопасных хранения и передачи цифровых данных транзакций между пользователями сети для совместного использования данных.

Уровень техники

Сегодня распределенные базы данных, основанные на протоколах блокчейн (в дальнейшей для краткости называемых просто "цепочками блоков"), используются для безопасной записи транзакций между двумя или более сторонами (например, между поставщиком и покупателем, между гражданином и государственным учреждением или банком и т.д.). Технологии, основанные на блокчейн, хорошо известны в данной области техники (см., например, "Mastering Bitcoin. Unlocking Digital Crypto-Currencies." Andreas M. Antonopoulos ("Осваиваем биткойн. Программирование блокчейна", Андреас М. Антонопулос), O'Reilly Media, 2014); вкратце их можно определить как постоянно растущие списки записей (блоков) данных, связанных в хронологическом порядке и защищенных с использованием криптографии; обычно записанные данные представляют собой транзакции.

Цепочки блоков в данной области техники управляются одноранговой сетью конечных вычислительных устройств (узлов) пользователей, следующих протоколу для связи между узлами: добавление новых блоков данных в цепочку блоков управляется соглашением между большинством узлов. Целостность и легитимность цепочек блоков, как правило, обеспечивается посредством выполнения добавления обманных блоков слишком затратным, с точки зрения затрат либо денег, либо времени.

Блокчейн наиболее распространенной технологии (блокчейн для криптовалюты биткоин) предусматривает запись всей информации, касающейся транзакции, в блоках ее цепочек неизменным образом: блок добавляется к цепочке блоков, только если он авторизован большинством узлов сети, и подлинность добавленного блока обеспечивается посредством криптографических функций (односторонних хеш-функций); вычисление функции является затратным, но верификационная проверка проводится быстро и легко с вычислительной точки зрения (например, в криптовалюте биткойн она реализуется неуправляемой верификационной сетью майнеров).

Известные в настоящее время протоколы блокчейн имеют два основных недостатка: во-первых, сеть верификации (сеть майнеров) цепочек блоков требует больших затрат энергии (сегодня потребление для верификационной проверки и управления 1/1000-ой банковских транзакций для биткойнов требует энергетического бюджета Ирландии); во-вторых, любой может принять в этом участие без сертификации, подтверждающей идентичность пользователя: возможен случай, когда одним и тем же пользователем создано и контролируется огромное количество учетных записей, что приведет к проблемам с безопасностью.

Сущность изобретения

Настоящее изобретение направлено на решение вышеуказанных проблем посредством реализуемой с помощью компьютера системы и реализуемого с помощью компьютера способа для безопасных совместного использования данных и хранения данных с использованием новой концепции блокчейна, называемой в данном документе "нейронный блокчейн" и подробно описанной ниже.

Изобретение дополнительно обеспечивает повышенную безопасность для хранения данных и совместного использования данных, преодолевая известные пределы систем аутентификации, основанных на именах пользователей и паролях, такие как, помимо прочего, потребность в огромном количестве различных и сложных паролей для повышения безопасности (личной) информации и риск того, что скопированные или взломанные пароли предоставят доступ к огромному объему указанной информации.

Кроме того, настоящее изобретение позволяет включить объекты, такие как пользователи сети для совместного использования данных. Физические объекты уже используются для создания, хранения и передачи данных, а в будущем будет формироваться еще больше связей между объектами и с их данными (Интернет вещей, (Internet of Things IoT) или Интернете всего). Однако известные с настоящее время системы для защищенного совместного использования данных не могут автономно управляться объектами вследствие отсутствия автоматически сертифицированной и доверительной идентичности указанных объектов и вследствие отсутствия способности указанных объектов взаимодействовать отличающимся образом при выполнении каждой отличающейся транзакции. Настоящее изобретение, таким образом, направлено также на решение этой проблемы, обеспечивая уникальное решение для аутентификации идентичности со слиянием физической и цифровой аутентификации.

Настоящее изобретение относится к реализуемой с помощью компьютера системе для безопасных хранения и передачи цифровых данных между пользователями сети для совместного использования данных, содержащей:

(a) множество вычислительных устройств для доступа пользователей к сети для совместного использования данных;

(b) цифровую идентичность, связанную с каждым пользователем сети и содержащую средства аутентификации, выполненные с возможностью автоматической (т.е. без вмешательства человека) выработки нового кода для аутентификации в ответ на каждый новый опрос для верификационной проверки идентичности;

(c) по меньшей мере один сертификационный объект, выполненный с возможностью аутентификации цифровой идентичности пользователей сети;

(d) по меньшей мере одну транзакцию между двумя или более пользователями сети, содержащую цифровую информацию, которая выработана по меньшей мере одним из указанных двух или более проверенных пользователей, принадлежит ему и/или находится в совместном использовании; и которая дополнительно содержит смарт-контракт, определяющий обязанности и права указанных двух или более проверенных пользователей в отношении цифровой информации; причем транзакция авторизована только в том случае, если цифровые идентичности указанных двух или более пользователей проверены указанным по меньшей мере одним сертификационным объектом;

(e) по меньшей мере один цифровой репозиторий, хранящий цифровую информацию транзакции и содержащий шлюз для совместного использования указанной цифровой информации, при этом безопасность доступа к указанной цифровой информации обеспечена цифровой идентификацией двух или более пользователей, вовлеченных в транзакцию: предпочтительно только указанные пользователи могут иметь доступ к цифровой информации (по меньшей мере к ее части), предпочтительно, как определено в смарт-контракте, который является частью транзакции;

(f) одну или более баз данных личного регистрационного учета на основе протокола типа блокчейн, связанных с каждым пользователем сети, предпочтительно, хранящихся в вычислительном устройстве пользователя или в цифровом виде соединенных с вычислительным устройством пользователя, и имеющих такую структуру, что, когда авторизована транзакция между двумя или более пользователями, в базы данных личного регистрационного учета, связанные с каждым из указанных двух или более пользователей добавлен новый блок, причем в указанном новом блоке только записаны цифровые адреса (гиперссылки) цифрового репозитория (цифровых репозиториев), хранящего (хранящих) цифровую информацию транзакции. Таким образом, в блоки баз данных личного регистрационного учета не записывается цифровая информация транзакции, которая хранится только в указанных одном или более цифровых репозиториях. База данных личного регистрационного учета пользователя содержит список цифровых репозиториев, хранящих цифровую информацию всех транзакций, в которые вовлечен указанный пользователь, а не саму цифровую информацию.

Изобретение также относится к реализуемому с помощью компьютера способу безопасных хранения и передачи цифровых данных между пользователями сети для совместного использования данных на основании реализованной на компьютере системе согласно изобретению, причем способ включает:

a) осуществление доступа пользователей посредством вычислительного устройства к сети для совместного использования данных;

b) представление сертификационному объекту транзакции между двумя или более пользователями сети;

c) аутентификацию сертификационным объектом цифровых идентичностей указанных пользователей, вовлеченных в транзакцию, и выдачу электронного сертификата вычислительным устройствам пользователя (пользователей), чья цифровая идентификация подтверждена;

d) авторизацию транзакции;

e) исполнение транзакции и сохранение цифровой информации транзакции в одном или более цифровых репозиториях;

f) добавление нового блока к базам данных личного регистрационного учета, связанным с каждым из пользователей, вовлеченных в транзакцию, причем в указанный новый блок записывают цифровые адреса указанных одного или более цифровых репозиториев, в которых сохранена цифровая информация транзакции.

Краткое описание чертежей

Далее будут описаны предпочтительные варианты осуществления настоящего изобретения со ссылкой на сопроводительные чертежи, на которых

на фиг. 1 представлен обзор элементов реализуемой с помощью компьютера системы (100) в соответствии с настоящим изобретением и их соединений;

на фиг. 2 представлен обзор элементов реализуемой с помощью компьютера системы, взаимодействующей при реализации способа согласно изобретению, согласно которому (фиг. 2A) транзакцию между двумя пользователями (103-1 и 103-2) предоставляют в сеть (101) посредством первого из указанных двух пользователей (103-1), и запрос на авторизацию транзакции отправляют сертификационному объекту (105), при этом сертификационный объект (105) таким образом опрашивает средства (114-1 и 114-2) аутентификации указанных двух пользователей; (фиг. 2B) транзакцию авторизуют посредством аутентификации цифровой идентичности (104-1 и 104-2) двух пользователей посредством сертификационного объекта (105), через их средства (114-1 и 114-2) аутентификации, и выдают электронный сертификат (113-1 и 113-2) каждому вычислительному устройству (103) проверенных пользователей (102'-1 и 102'-2);

на фиг. 3 представлен обзор элементов реализуемой с помощью компьютера системы, взаимодействующей при реализации способа согласно изобретению, согласно которому оба новых блока (118), добавленных в базы (108-1 и 108-2) данных личного регистрационного учета первого и второго проверенных пользователей (102'-1 и 102'-2), вовлеченных в транзакцию (106-1), содержат ссылку (например, ги-

перссылку) (109) на цифровой репозиторий (107-1), в котором хранится цифровая информация указанной транзакции (106-1); показано, что база (108-2) данных личного регистрационного учета второго пользователя также содержит предшествующий по времени блок, который содержит вторую ссылку (109') на второй цифровой репозиторий (106-2), хранящий цифровую информацию второй транзакции (106-2) между указанным вторым пользователем (102'-2) и третьим пользователем (не показан); при этом эта же вторая гиперссылка (109') таким образом записана в блоке базы (108-3) данных личного регистрационного учета указанного третьего пользователя;

на фиг. 4 показан предпочтительный вариант осуществления изобретения, в котором цифровой репозиторий (107-1), хранящий цифровую информацию транзакции (106-1), также является проверенным пользователем (102'-5) сети, имеющим свою собственную цифровую идентичность (104-5) и являющимся источником для новой базы (108-5) данных личного регистрационного учета, в которой записаны транзакции, в которые вовлечен указанный цифровой репозиторий (107-1);

на фиг. 5 показаны приведенные для примера базы данных личного регистрационного учета в соответствии с изобретением, имеющие (A) линейную структуру, когда блоки связаны хронологически, или (B) древовидную структуру, при которой блоки (также) семантически связаны, и которая является разветвленной, например, на основе различных рассматриваемых дел пользователя или аватаров разных пользователей, или выдается исходя из смарт-контракта, требующего различных параллельных цепочек блоков, основанных на разных правах или различных организационных процедурах;

на фиг. 6 показаны средства аутентификации типа отличительной метки в соответствии с предпочтительным вариантом осуществления настоящего изобретения: отличительная метка может иметь различные формы, видимые невооруженным глазом, (A), при освещении оптического измерительного устройства на разных длинах волн (B) или при анализе при различных разрешениях (C), или она может обеспечить различные значения в одних и тех же точках при измерении с помощью различных измерительных устройств (D) или протоколов/условий;

на фиг. 7 показаны транзакции примера 4.

Осуществление изобретения

Согласно изобретению сеть (101) для совместного использования данных может иметь любую топологию и/или структуру сети связи; в предпочтительном варианте сеть является Интернетом.

Каждый из элементов реализуемой с помощью компьютера системы (100) соединен с другим элементом через любые подходящие проводные и/или беспроводные средства, выполненные с возможностью сообщения и передачи цифровых данных между указанными элементами и через сеть; в предпочтительном варианте элементы системы (100) были соединены беспроводными средствами.

"Пользователь", как определено в настоящем документе, является субъектом, осуществляющим доступ к сети для совместного использования (101) данных посредством вычислительного устройства (103). Например, пользователь может быть человеком, использующим вычислительное устройство, или он может быть объектом, содержащим вычислительное устройство (соединенное с указанным объектом или встроенное в него). В предпочтительных вариантах осуществления изобретения по меньшей мере один из пользователей сети является объектом, содержащим вычислительное устройство, предпочтительно объектом с искусственным интеллектом.

В соответствии с настоящим изобретением каждый пользователь сети имеет физическую и цифровую ("фигитальную", phygital) идентичность (104), посредством которой обеспечена однозначная идентифицируемость указанного пользователя; в соответствии с настоящим изобретением каждый пользователь, таким образом, взаимно однозначно связан с цифровой идентичностью, которая является конкретной для каждого пользователя.

Термин "взаимно однозначно" означает взаимно однозначное соответствие; например, упоминание пользователя и его цифровой идентичности означает, что для указанного пользователя существует одна и только одна цифровая идентичность, и что каждая конкретная цифровая идентичность идентифицирует одного и только одного пользователя.

"Цифровая идентичность" (104) пользователя характеризуется тем, что она содержит средства (114) аутентификации для однозначной аутентификации идентичности пользователя.

"Средства (114) аутентификации" являются любыми средствами, выполненными с возможностью выработки и передачи кода для аутентификации (такого как, без ограничения, ключ или пароль), подлежащего верификации для проверки идентичности пользователя.

Средства (114) аутентификации могут быть библиотекой цифровых и/или аналоговых значений, а код для аутентификации может быть составлен из случайной строки из подмножества указанных цифровых и/или аналоговых значений. Согласно изобретению указанный код для аутентификации верифицируется сертификационным объектом (105): в ответ на каждый новый опрос, выполняемый сертификационным объектом (105), средства (114) аутентификации вырабатывают новый код для аутентификации (отличный от любого предыдущего кода для аутентификации, выработанного средствами аутентификации).

В предпочтительном варианте цифровая идентичность (104) пользователя (102) включает в себя публичное имя пользователя.

При необходимости цифровая идентичность (104) пользователя (102) содержит один или более аватаров, все из которых связаны с одним и тем же средством аутентификации. "Аватар" для данного пользователя может быть, например, дополнительным именем пользователя, используемым для определенного типа транзакции, что позволяет выполнить сертификацию с помощью средств (114) аутентификации цифровой идентичности, гарантируя конфиденциальность.

Когда код для аутентификации, выработанный с помощью средств (114) аутентификации, аутентифицирован (подтверждена его подлинность) сертификационным объектом (105), цифровая идентичность пользователя подтверждается, и выдается электронный сертификат (113) (см. фиг. 2); пользователь является "проверенным пользователем", чьей идентичности (проверенной и сертифицированной) можно доверять.

"Транзакция" (106) между двумя или более пользователями (102) сети (101) содержит цифровую информацию, которая выработана по меньшей мере одним из указанных двух или более проверенных пользователей, принадлежит ему и/или находится в совместном использовании.

Например, транзакция содержит указанную цифровую информацию между двумя или более пользователями или заключается в ее совместном использовании.

"Цифровая информация" в контексте настоящего изобретения может быть (необработанными или обработанными) данными, программой, смарт-контрактом или способом выражения/представления значений (например, биткойнов или других криптовалют, но это не является исчерпывающим).

В соответствии с настоящим изобретением транзакция (106) авторизована только тогда, когда проверена подлинность цифровых идентичностей (104) указанных двух или более пользователей (102).

Таким образом, в отличие от баз данных, основанных на протоколах блокчейн в данной области техники, согласно которым транзакцию авторизуют по согласию сети контроля (например, по способу доказательства выполнения работы для обменов криптовалюты биткоин), транзакции (106) в реализуемой с помощью компьютера системе (100) согласно изобретению авторизуют посредством верификации цифровых идентичностей (104) пользователей (102), вовлеченных в транзакцию, посредством аутентификации средств (114) аутентификации их цифровой идентичности с помощью сертификационного объекта (105). В предпочтительном варианте авторизацию транзакции передают в сеть.

В качестве простого примера, сертификационный объект (105) может быть банком или правительством, который или которое разрешает транзакцию (106) между двумя проверенными пользователями (102') для продажи/покупки товара.

В предпочтительном варианте компьютерная система (100) содержит несколько сертификационных объектов (105), при этом каждый сертификационный объект выполнен с возможностью авторизации или разрешения транзакции конкретного типа.

В частном случае сертификационный объект (105) может сам являться пользователем (102) сети (101), вовлеченным в данную транзакцию (106): в качестве примера, когда транзакция, или сделка, (106-1) включает в себя продажу/покупку товара между двумя пользователями (102-1 и 102-2), сертификационный объект (105-1), который разрешает указанную транзакцию (106-1), может сам быть вовлечен в дополнительную транзакцию (106-2) с указанными двумя пользователями, например, для уплаты налогов на продажу/покупку указанного или иного товара: в этом случае дополнительный сертификационный объект (105-2) может аутентифицировать цифровую идентичность (104-1) первого сертификационного объекта (105-1), вовлеченного в дополнительную транзакцию (106-2) в качестве пользователя.

В соответствии с изобретением цифровая информация транзакции (106) хранится по меньшей мере в одном цифровом репозитории (107) (см. фиг. 3).

"Цифровой репозиторий" (107) представляет собой любой носитель или цифровую систему, выполненный или выполненную с возможностью хранения цифровой информации. Примерами подходящих цифровых репозиториев являются: жесткий диск, облако, "туман", ключ USB и т.д. Цифровой репозиторий может быть соединен с другими цифровыми репозиториями через сеть для совместного использования данных, такой как Интернет.

В предпочтительном варианте осуществления безопасность цифрового репозитория (107), который хранит цифровую информацию транзакции между двумя или более пользователями (102), обеспечивается цифровыми идентичностями (104) из указанных двух или более пользователей (102), так что только проверенные пользователи (102'), вовлеченные в транзакцию (106), могут получить доступ к указанным одному или более цифровым репозиториям (107), в которых хранится цифровая информация указанной транзакции (106).

Имея доступ к цифровой информации, хранящейся в одном или более цифровых репозиториях (107), проверенные пользователи (102'), вовлеченные в транзакцию (106), способны считать указанную информацию; в предпочтительном варианте проверенные пользователи (102') не могут изменить цифровую информацию.

В предпочтительном варианте сертификационный объект (105), который аутентифицирует цифровую идентичность пользователя и который не является пользователем транзакции, не имеет доступа к цифровой информации, выработанной указанным пользователем, принадлежащей ему или находящейся в совместном использовании указанного пользователя.

При необходимости цифровая информация транзакции может быть сохранена в туманной базе данных (например, вместо облачной базы данных или локального носителя для хранения данных), так что разные части цифровой информации хранятся в разных цифровых репозиториях.

В предпочтительном варианте цифровая информация транзакции распространена в нескольких цифровых репозиториях, по возможности в одном отличающемся репозитории для каждого пользователя, вовлеченного в транзакцию.

При необходимости транзакция содержит смарт-контракт или заключается в смарт-контракте, который определяет обязанности и права вовлеченных пользователей по цифровой информации транзакции. Например, смарт-контракт может определять, какой пользователь имеет доступ к какой цифровой информации транзакции. Пользователи (102) транзакции (106) могут таким образом иметь доступ только к одному или более цифровым репозиториям (107), хранящим цифровую информацию, но не ко всем, имея при этом доступ только к части указанной цифровой информации, как определено в смарт-контракте. Предварительно определенные шаблоны смарт-контрактов могут быть использованы для определения прав и обязанностей пользователей.

Доступ к цифровой информации может быть публичным или частным, как это определено, например, в смарт-контракте.

Цифровой адрес цифровых репозиториев (107), в которых хранится по меньшей мере часть информации транзакции (106), записывается в блоках баз (108) данных личного регистрационного учета, связанных с каждым пользователем транзакции (см. фиг. 3), предпочтительно в виде гиперссылки или в любой другой подходящей форме, которая может создать соединение с цифровым репозитории.

Базы (108) данных личного регистрационного учета реализуемой с помощью компьютера системы (100) согласно изобретению основаны на протоколе типа блокчейн, поскольку в них совместно используются некоторые, но не все из типичных особенностей цепочки блоков: базы (108) данных личного регистрационного учета в соответствии с изобретением действительно представляют собой растущий список блоков, которые включают в себя криптографический ключ (например, хеш-функцию), который связывает каждый новый блок с предыдущим, и временную метку. Однако они отличаются от типичных известных в данной области техники цепочек блоков по меньшей мере тем, что в блоки записывают не цифровую информацию транзакции (106), а только адрес репозиториев (107), в которых хранится указанная информация, и тем, что добавление новых блоков (118) управляется не одноранговой сетью узлов, а посредством проверки подлинности цифровых идентичностей (104) пользователей с помощью сертификационного объекта (105), как описано выше.

При необходимости блоки базы (108) данных личного регистрационного учета могут быть (также) семантически связаны, когда они содержат один и тот же хэштег, ключевое слово, число или строку, при необходимости под управлением посредством специализированного аватара. Например, все блоки базы (108) данных личного регистрационного учета одних и тех же или разных пользователей (102), относящихся к банковским транзакциям, могут быть связаны общим хэштегом (например, #bank), что таким образом делает их всех доступными для поиска по этому общему хэштегу. В качестве дополнительного примера, все блоки, относящиеся к денежным транзакциям на одну и ту же сумму, могут быть доступны для поиска по указанной сумме (т.е. по определенному числу). База (108) данных личного регистрационного учета одного и того же пользователя (102) может таким образом иметь линейную форму (см. фиг. 5A), когда блоки связаны только хронологически, или они могут иметь древовидную форму (см. фиг. 5B), когда блоки (также) организованы семантически.

В предпочтительном варианте базы данных личного регистрационного учета являются частными и не доступны пользователям, не вовлеченным в транзакцию, а цифровая информация транзакции, хранящаяся в цифровом репозитории, адрес которого записан в базу данных личного регистрационного учета, является частной и доступна только по меньшей мере одному из проверенных пользователей, вовлеченных в транзакцию.

В предпочтительном варианте осуществления транзакция (106) содержит смарт-контракт, который включает в себя форму представления данных о пользователях, вовлеченных в транзакцию, реализуемая с помощью компьютера система (100) выполнена так, что, когда указанная транзакция (106) авторизована, хэштег, который идентифицирует тип транзакции, вырабатывается автоматически в базах (108) данных личного регистрационного учета указанных вовлеченных пользователей.

Боковая цепочка (также известная как "дочерняя цепочка") представляет собой отдельную цепочку блоков, которая присоединена к своей родительской (или основной) цепочке блоков с использованием двойной фиксации (two-way peg). Двойная фиксация обеспечивает взаимозаменяемость активов с заданной скоростью между родительской цепочкой и боковой цепочкой. Боковые цепочки были разработаны с целью повышения уровня безопасности и расширения масштабов цепочек блоков.

Ясно, что система с боковыми цепочками может быть легко реализована в системе согласно изобретению. Например, одна или более боковых цепочек могут быть прикреплены к базе данных личного регистрационного учета системы согласно изобретению, что таким образом делает их соединенными с одним и тем же цифровым репозиторием (одними и теми же цифровыми репозиториями).

Таким образом, реализованная на компьютере система (100) согласно изобретению предпочтитель-

но дополнительно содержит одну или более боковых цепочек, прикрепленных к одной или более базам (108) данных личного регистрационного учета, связанным с пользователями (102) сети (101).

Система согласно изобретению, в которой цифровая информация записывается в репозиторий, а не в саму цепочку блоков (базу данных личного регистрационного учета), позволяет избежать риска ослабления цепочки блоков посредством прикрепления к слабой боковой цепочке, что является недостатком боковых цепочек системы, известных в данной области техники.

Когда пользователь является объектом, предпочтительными сертификационными объектами могут быть, без ограничения, производитель объекта и/или владелец объекта.

В соответствии с предпочтительными вариантами осуществления изобретения цифровые репозиторий (107) и одни и те же сертификационные объекты (105) могут также быть пользователями этой сети (101). В предпочтительном варианте, когда цифровой репозиторий (107-1), хранящий цифровую информацию первой транзакции (106-1), является проверенным пользователем (102'-5) дополнительной транзакции, (первый или новый) блок может быть выработан в базе (108-5) данных личного регистрационного учета, связанной с цифровым репозиторием (см. фиг. 4).

Когда пользователь сети (101) является цифровым репозиторием (107) для удаленного хранения цифровой информации, таким как облачный сервер, один из сертификационных объектов (105) может быть, без ограничения, поставщиком указанного цифрового репозитория. Если такому поставщику причитается комиссия, он также может быть напрямую вовлечен в транзакцию в качестве пользователя.

Цифровой репозиторий (107) в соответствии с настоящим изобретением также может выступать в качестве сертификационного объекта (105), выполненного с возможностью аутентификации цифровой идентичности пользователя.

Цифровая идентичность может быть придана также файлам, хранящимся в репозитории: например, цифровая идентичность файла может содержать имя файла и средства аутентификации цифровой идентичности репозитория, в котором хранится файл.

В соответствии с предпочтительными вариантами осуществления, средства (114) аутентификации реализуемой с помощью компьютера системы (100) согласно настоящему изобретению являются аппаратными средствами с маркером или аппаратными средствами с физически неклонируемой функцией (Physical Unclonable Function, PUF) или шаблоном по концепции SIMPL (SIMulation Possible but Laborious) ("моделирование возможно, но трудоемко") и аппаратно реализуемыми функциональностями криптографических примитивов. В наиболее предпочтительных вариантах осуществления средствами аутентификации является отличительная метка, содержащая множество точек, имеющих измеримые свойства материала, а также содержащая процессор, выполненный с возможностью исполнения протокола, в соответствие с которым вырабатывают код для аутентификации посредством шифрования значений, полученных путем измерения по меньшей мере одного из указанного измеримых свойств материала в одной или более точках отличительной метки посредством измерительного устройства.

"Измеримое свойство материала" представляет собой любое аналогичное свойство, которое можно измерить, такое как любое физическое или химическое свойство, и измерение которых возвращает значение. Например, измеримыми свойствами материала отличительной метки могут быть оптические, электрические, топографические, механические, тепловые, магнитные, химические свойства и комбинации указанного.

Отличительная метка в соответствии с предпочтительными вариантами осуществления изобретения является таким образом библиотекой значений, получаемых путем измерения одного или более свойств ее материала в одной или более точках отличительной метки; отличительная метка может вырабатывать коды для аутентификации, состоящие из случайной строки из указанных значений. Код для аутентификации может, таким образом, быть выработан посредством измерения свойств материала подмножества точек, получения значений, комбинирования случайным образом строки указанных значений и преобразования ее в код с помощью алгоритма. Например, для каждой точки отличительной метки могут быть получены от 100 до 10000 различных значений.

В предпочтительном варианте указанная отличительная метка имеет примерно до 106 точек, более предпочтительно от 100 до 106 точек, на квадратный миллиметр, имеющих различные измеримые свойства материала. По существу, новый код для аутентификации пользователя (одноразовый ключ/пароль) может быть выработан при каждом взаимодействии. Уникальный пароль составлен из положений используемых точек с учетом методологии считывания и значений свойств материалов в каждой из измеренных точек. Эти значения затем могут быть скремблированы посредством программных способов шифрования, с тем чтобы повысить сложность и еще больше приблизиться к устойчивому уровню безопасности квантовых вычислений.

WO 2015140731 раскрывает тонкие пленки (метки), полученные путем химического осаждения из паровой фазы с использованием лучей (chemical beam vapor deposition, CBVD), подходящие в качестве средства аутентификации по отличительной метке в соответствии с настоящим изобретением. На указанных тонких пленках может быть одновременно сформирован конфигурационный узор, который может быть считан при разных масштабах для обеспечения получения широкой группы различных свойств материалов (конфигурационные узоры с разрешением от нано- до (суб) миллиметрового диапазона,

сверхскрытая (ultra-covert) функция, см., например, на фиг. 7); производственный процесс, раскрытый в WO 2015140731, позволяет получить более 1020 различных конфигураций в одном и том же процессе осаждения, что таким образом потенциально приводит более чем к 1020 различных цифровых идентичностей, содержащих указанные тонкие пленки в качестве средств аутентификации. С таким огромным количеством комплексных значений, встроенных в пленку, отличительная метка обеспечивает неклонируемую электронную идентичность пользователей, так как ее невозможно подделать даже с очень большими затратами, не зная точную конфигурацию оборудования и все параметры процесса, используемого для выращивания тонких пленок. Это делает невозможным подделку пленки методом обратного инжиниринга. Посредством измерения и комбинирования такого большого количества измеримых свойств материала, можно выработать огромное количество различных кодов аутентификации с помощью одной отличительной метки. Коды для аутентификации, выработанные отличительной меткой, причем новый код вырабатывается при каждом опросе, могут быть вставлены в шлюзы для предотвращения нежелательного удаленного доступа, например, к цифровому репозиторию.

Изменчивость свойств материала в зависимости от оказываемого на него воздействия, математических алгоритмов (переменной прошивки, используемой в качестве кода шифрования) или различных используемых измерительных устройств обеспечивает очень большое количество возможных значений и комбинаций значений, получаемых с помощью одной и той же отличительной метки. Опрос, выполняемый сертификационным объектом, может изменяться по любому параметру с бесконечным количеством возможных ответов, выходящих за рамки того, что может быть сохранено в программной базе двоичных данных. Отличительная метка таким образом в ответ на каждый запрос может выработать новый код, который невозможно спрогнозировать. Таким образом, каждая транзакция может быть однозначно аутентифицирована и сертифицирована.

В предпочтительном варианте отличительная метка изобретения является пленкой, полученной путем химического осаждения из паровой фазы с использованием лучей (chemical beam vapor deposition, CBVD). Известно, что оксиды, которые могут быть нанесены с помощью процесса CBVD, обладают многофункциональными свойствами (т.е. одновременными различными свойствами), которые легко настраиваются путем незначительных модификаций состава материала и процесса осаждения. Предпочтительные оксиды, используемые в процессе CBVD для производства пленки содержат TiO_2 (оксид титана), HfO_2 (оксид гафния), ZrO_2 (оксид циркония), Al_2O_3 (оксид алюминия), SiO_2 (диоксид кремния), ZnO (оксид цинка), TaO_5 (оксид тантала (V)), оксиды ванадия, Nb_2O_5 (оксид ниобия (V)), $LiNbO_3$ (ниобат лития), $LiTaO_3$ (танталат лития).

В предпочтительном варианте в компьютерной системе согласно изобретению цифровая идентичность, взаимно однозначно связанная с каждым пользователем, содержит уникальную отличительную метку.

"Уникальная" в отношении отличительной метки означает, что отличительная метка цифровой идентичности, связанной с данным пользователем, отличается от отличительной метки цифровой идентичности, связанной с другим пользователем; например, отличительная метка является уникальной, когда она отличается от других отличительных меток по меньшей мере по одному из своих измеримых свойств материала и/или по меньшей мере по одному из значений, полученных при измерении одного или более его измеримых свойств материала в данной точке. Например, в данной точке с координатами x, y могут быть измерены одно или более свойств материала с получением конкретного значения, которое является уникальным для указанной точки/свойства для данной отличительной метки. Более того, комбинация указанных значений может обеспечивать получение строки значений, уникальной для каждой отличительной метки.

В предпочтительном варианте уникальная отличительная метка помещается с пакетированием в устройство для обеспечения уникальной идентичности (либо инструмент в виде аватара личности, либо независимое автономное устройство).

В предпочтительном варианте компьютерная система дополнительно содержит по меньшей мере одну двойную отличительную метку, связанную с каждой отличительной меткой. "Двойная отличительная метка" является идентичной копией отличительной метки, измеримые свойства материала которой идентичны измеримым свойствам материала отличительной метки, с которой двойная отличительная метка связана в каждой точке. В предпочтительном варианте реализуемая с помощью компьютера система согласно изобретению содержит одну двойную отличительную метку для каждой отличительной метки каждого пользователя; при необходимости компьютерная система согласно изобретению содержит две или более копий двойной отличительной метки.

Двойная отличительная метка в соответствии с предпочтительными вариантами осуществления изобретения содержит процессор, выполненный с возможностью сообщения с отличительной меткой, с которой она связана, и расшифровки кода для аутентификации, выработанного отличительной меткой пользователя. Каждая двойная отличительная метка предпочтительно выполнена с возможностью сообщения с отличительной меткой, с которой она связана, с помощью уникального языка, на основе уникального шифрования значения, специфичного для каждого отличительной метки, и расшифровки двойной отличительной метки.

В предпочтительном варианте реализуемая с помощью компьютера система согласно изобретению содержит множество двойных отличительных меток для каждой отличительной метки для резервирования и/или для повышения устойчивости и точности при считывании/измерении свойств указанной отличительной метки, или недопущения чрезмерного открытия единственного сервера для массовых опросов.

В предпочтительных вариантах осуществления настоящего изобретения сертификационный объект (105) является удаленным центральным репозиторием аппаратного типа, имеющим цифровое соединение со средствами аутентификации отличительных меток цифровых идентичностей пользователей; в более предпочтительном варианте в нем хранятся двойные отличительные метки, связанные с указанными отличительными метками; при необходимости одна или более копий двойной отличительной метки хранятся в разных центральных репозиториях аппаратного типа: аналоговых запоминающих устройствах, не являющихся перезаписываемыми и не имеющих двоичного кодирования.

При необходимости сертификационный объект, хранящий двойную отличительную метку и выполненный с возможностью выдачи электронного сертификата аутентичности при проверке отличительной метки, может в цифровой форме сообщаться с другими сертификационными объектами и передать сертификат на указанные другие сертификационные объекты.

Двойные отличительные метки могут быть сохранены в единственной базе данных, или несколько независимых систем могут перегруппировать меньшее количество отличительных меток, выступающих в качестве узла, при этом различные узлы соединены одной и той же системой с отличительной меткой, а процедура аутентификации реализуется за счет транзитивности с переходом от узла к узлу до тех пор, пока не будет установлено соединение между всеми различными отличительными метками пользователей.

Сертификационный объект предпочтительно выполнен с возможностью исполнения протокола аутентификации для аутентификации отличительной метки, который включает: опрос отличительной метки с получением кода для аутентификации, дешифровку указанного кода для аутентификации посредством двойной отличительной метки, подтверждение аутентификации отличительной метки и выдачу сертификата аутентификации.

Отличительная метка и ее двойная отличительная метка также могут быть использованы в способе шифрования, наподобие такого, для которого используются шифровальные книги, на основании библиотеки свойств материала отличительной метки, согласно которому две (или более) идентичные отличительные метки (отличительную метку пользователя и одну двойную отличительную метку или большее количество двойных отличительных меток) используют в качестве ключей шифрования "чистых аппаратных средств".

Подход с двойными отличительными метками обеспечивает несколько преимуществ:

первое обеспечивает методологию симметричного шифрования без необходимости использования ресурсоемкого (аппаратного и энергоемкого) программного подхода при решении проблемы передачи ключей симметричного шифрования;

второе позволяет избегать использования любого вида цифровой базы данных для хранения, которая может быть взломана и скопирована (оцифровкой), поскольку отличительная метка так сложна и может обеспечить такое большое количество различных ключей, что их невозможно просто воспроизвести на цифровом уровне.

По меньшей мере четыре сферы параметров могут создавать очень сложные комбинации значений для выработки ключа:

различные комбинации точек (20-50 свойств, извлеченных из точек в количестве от 10000 до 1 миллиона);

недвоичное кодирование с потенциально более чем 1000 различных значений при считывании для каждой точки;

различные протоколы чтения с выработкой различных значений: в качестве примера, для оптического считывания комбинация 3 разных длин волн, каждая из которых имеет 10 уровней интенсивности, приводит к 1000 доступных спектров, но если достигается 100 различных уровней интенсивности, получается 1 миллион различных спектров; при этом каждый спектр обеспечит уникальный набор значений для одних и тех же точек;

дискретизация непрерывных аналоговых значений в переменном количестве интервалов: для 1000 различных значений может быть 1000 различных способов зафиксировать взаимно однозначную связь между измеренным значением и используемым значением в базе данных.

Таким образом, количество комбинаций просто удивительно и не фиксировано раз и навсегда. Следовательно, ключи являются уникальными и не могут быть скопированы, даже если их правила доступны физически.

Наиболее важным моментом является то, что этот цифровой совместимый протокол не обязательно должен поддерживаться каким-либо оборудованием на физическом уровне для правил, а вспомогательное оборудование может быть обеспечено самим внешним считывателем (например, смартфоном).

В предпочтительных вариантах осуществления отличительные метки выполнены пакетированными с измерительным устройством (в виде однокристальных систем) или выращены с получением монолит-

ной структуры на измерительном устройстве, выполненном с возможностью измерения указанного по меньшей мере одного измеримого свойства материала.

Отличительные метки в соответствии с предпочтительными вариантами осуществления изобретения могут дополнительно быть выполнены с возможностью шифрования и дешифровки информации. Например, отличительная метка цифровой идентичности пользователя может быть использована в качестве криптографических средств, обеспечивающих возможность шифрования цифровой информации, хранящейся в цифровом репозитории, расшифровка которой может быть выполнена только посредством двойной отличительной метки.

На физическом уровне доказательство идентичности уже доступно для граждан с помощью паспортов и/или удостоверений личности. Они позволяют выезжать за границу, удостоверять личность для различных ведомств или государственных служащих (банков, нотариусов и т.д.) с известными преимуществами.

На цифровом уровне универсальная сильная ориентированная на пользователя идентичность, обеспечивающая прослеживаемость и аутентификацию пользователя, больше не является инструментом, который хорошо бы иметь, а является инструментом, который обязательно нужно иметь.

1. Она обеспечит хорошо регулируемые взаимодействия, что означает:

a) значительное сокращение спама и вредоносных программ-вымогателей;

b) поддержку бизнеса/транзакций/взаимодействия/социальных сетей без являющихся посредниками доверенных платформ, контролирующих данные граждан;

c) поддержку универсальных стандартных протоколов;

d) обеспечение смарт-контрактов с беспрецедентными функциями.

2. Создание личной платформы/базы данных ERP (Enterprise Resource Planning, планирования ресурсов предприятия) позволит:

a) избежать расходящегося количества параллельных цифровых идентичностей;

b) легко и эффективно сортировать, систематизировать и управлять собственными данными;

c) осуществлять самостоятельное управление сертификатами, позволяющее быстро и легко передавать их между объектами.

3. Обеспечение для пользователя возможности иметь инструмент VRM (Vendor Relation Management, управление взаимоотношениями с поставщиками) для улучшения взаимодействия с бизнесом:

a) обеспечение возможности передачи прав на личные данные третьим сторонам;

b) прослеживание и проверка того, как используются собственные данные;

c) получение платежей за собственные данные в целях получения прибыли.

Схожие преимущества также могут быть получены для ведения хозяйственной деятельности. Можно упомянуть дополнительные преимущества, такие как:

1. Защита бренда:

a) простота управления товарными знаками и их проверка на всех уровнях, поскольку может быть доступна единая платформа (или единый интерфейс, выполненный с возможностью соединения всех платформ).

2. Защита интеллектуальной собственности:

a) заявленный приоритет,

b) уменьшение затрат за счет повышения функциональной совместимости и общих новых стандартов.

3. Более гибкое планирование ресурсов предприятия, позволяющее соединить разные компании и коммерческие отделы.

4. Уменьшение количества посредников и поддержка проверки дипломов/сертификатов.

5. Уменьшение административной нагрузки.

6. Сохранение управления собственными данными и критически важной информацией и их независимости, устраняя посредников, с надежным контролем важных данных.

Что касается правительств, то указанное может обеспечить огромное количество улучшений для снижения затрат и повышения безопасности их услуг. Помимо прочего можно упомянуть следующие:

1. Борьба с мошенничеством и уклонением от уплаты налогов:

a. обеспечение цифровых налогов, не основанных на фиксированной ставке.

2. Управление транснациональными услугами (помимо прочего, охрану здоровья путешествующих граждан).

3. Более гибкое управление голосованием и гражданским волеизъявлением.

4. Обеспечение большей безопасности граждан.

Упрощение цифровизации (в том числе для пожилых людей) и получение общества, более вовлеченного в цифровую сферу.

Все из следующего: проверенных пользователей (102'), вовлеченных в данную транзакцию (106), цифровых репозиториев (107), хранящих информацию указанной транзакции (106), блоков книг (108) личного регистрационного учета пользователей, в которых записаны цифровые адреса указанных цифровых репозитории (107), связаны вместе в реализуемой с помощью компьютера системе согласно изобре-

тению. В частности, базы (108) данных личного регистрационного учета реализуемой с помощью компьютера системы (100) согласно настоящему изобретению связаны тем, что называется в настоящем документе "нейронные связи": каждый из блоков книг (108) личного регистрационного учета различных пользователей, в которых записана одна и та же гиперссылка по меньшей мере на один цифровой репозиторий (107), хранящий цифровую информацию данной транзакции (106) между указанными различными пользователями, связаны друг с другом тем, что называется в настоящем документе "внешняя нейронная связь" (109, фиг. 3). Кроме того, в соответствии с предпочтительными вариантами осуществления изобретения блоки баз данных личного регистрационного учета одних и тех же или различных пользователей могут быть семантически связаны "внутренней нейронной связью" (110) (см. на фиг. 5B).

(Внутренние и/или внешние) нейронные связи, которые соединяют блоки баз данных личного регистрационного учета в компьютерной системе согласно изобретению, образуют то, что в настоящем документе называется "нейронной цепочкой блоков".

Взаимосвязь баз данных личного регистрационного учета компьютерной системы дополнительно связывает всех пользователей, имеющих доступ к сети для совместного использования данных, идентичность которых сертифицирована. Фактически, каждая новая нейронная связь создается только после авторизации транзакции, таким образом, после аутентификации цифровых идентичностей пользователей транзакции. Таким образом, каждая нейронная связь вносит вклад в укрепление протокола аутентификации для вовлеченных пользователей и доверие к базе данных личного регистрационного учета каждого пользователя, которые могут быть сделаны количественными.

Аутентификация цифровых идентичностей пользователей в соответствии с настоящим изобретением создает независимые доверительные отношения между группами пользователей сети, вовлеченных в транзакцию; чем больше увеличивается количество транзакций между пользователями сети (и, следовательно, количество проверенных пользователей), тем больше растет сеть доверенных (проверенных) пользователей. Система согласно изобретению повышает безопасность на уровне как физической, так и цифровой аутентификации; объединение физической и цифровой идентичности обеспечивает уникальную универсальную стандартную систему аутентификации, которая не зависит от управляющих объектов, однако является проверенной благодаря совместному партнерству, в которое вовлечены все, от правительства до бизнеса, вплоть до людей и объектов; более того, она доступна каждому, при условии наличия у участника "фигитальной" идентичности.

Уровень доверия также может быть экстраполирован по подкатегориям (семантический подход) в зависимости от количества нейронных связей, поддерживающих пользователя в такой подкатегории.

В предпочтительном варианте осуществления согласно изобретению, когда выполняется транзакция, выдается смарт-контракт. Фиксированный шаблон смарт-контракта, отсортированный между различными предварительно определенными шаблонами (новые шаблоны могут еще быть выработаны путем общего консенсуса и сделаны доступными), может определить информацию, которая загружена в цифровой репозиторий. Например, в шаблоне смарт-контракта может быть указан широкий диапазон различных параметров/индикаторов, таких как тип контракта (например, транзакция продажи), предыдущий владелец (продающая сторона), новый владелец (покупающая сторона), объект (идентифицированный отличительной меткой), правительство, которому уплачен НДС или уплачен налоги, владелец (владельцы) (также идентифицированный (идентифицированные) отличительной меткой) цифрового хранилища, в котором смарт-контракт зарегистрирован, возможно, различные банки, осуществляющие поддержку транзакции и, возможно, столько пользователей, сколько необходимо для обеспечения безопасности и проведения транзакции. На финансовом уровне могут быть определены различные суммы обмена. Сертификационные объекты могут иметь доступ к информации смарт-контракта - как это определено контрактом - или по возможности будут просто наблюдать сертифицирующие идентичности третьих сторон, но без доступа к информации для укрепления доверия к транзакции. Затем двойная база данных может создать новые блоки во всех соответствующих книгах личного регистрационного учета различных пользователей с "семантическим" подходом (тегированием), как это предусмотрено шаблоном. Например, в предыдущей транзакции будет создан блок в базе данных личного регистрационного учета продающей стороны (цепочка блоков для бухгалтерского учета). В такой блок не вводится никакой информации, а создается зашифрованная гиперссылка, указывающая на цифровой репозиторий. Каждый из репозиториев является также полностью независимым от друг друга, и информация, хранящаяся в нем, может быть доступна/изменена только путем выработки нового кода посредством соответствующей отличительной метки, если пользователю было позволено сделать это. Изменение информации может быть предпочтительно обработано путем выработки нового блока с использованием первого репозитория в качестве корня/источника такой новой базы данных регистрационного учета. Различные параллельные базы данных регистрационного учета могут быть выпущены для каждого индикатора в смарт-контракте и организованы семантически или по другим правилам, введенным в смарт-контракте.

База данных личного регистрационного учета может принять инструкцию по созданию блока посредством какого-либо смарт-контракта, в который она вовлечена, как только аутентификация будет подтверждена, и будет, таким образом, соединена с многими различными цифровыми репозиториями в соответствии с ранее раскрытым протоколом полностью автоматизирован образом (см. фиг. 7).

Компьютерная система согласно изобретению позволяет соединять различные вертикали и создает сеть третьего поколения, содержимое которой является полностью отслеживаемым и сертифицируется ее собственными пользователями без какого-либо управления, обеспечиваемого ограниченным количеством контролирующих сертифицирующих органов (сертификационных объектов). Реализуемая с помощью компьютера система (100) согласно изобретению такова, что соединения между ее элементами могут образовывать сеть (101) для совместного использования данных, которая является Интернетом вещей или Интернетом всего.

Кроме того, базы данных личного регистрационного учета согласно изобретению обеспечивают запись транзакций, для которых требуется гораздо меньше места для хранения по сравнению с типичными цепочками блоков, поскольку в них записываются только адреса цифровых репозиториев, в которых фактически хранится цифровая информация. В предпочтительном варианте цифровые репозитории создаются в небольшом количестве, в основном для целей резервного копирования.

Например, в случае нарушения связанности базы данных личного регистрационного учета пользователя цифровые репозитории могут быстро и независимо создать новую копию. В таком аспекте нейронный блокчейн очень устойчив к взлому даже в автономном процессе, и каждый отдельный блок действует как независимый объект (должен быть взломан индивидуально, чтобы получить доступ к информации).

В предпочтительном варианте, если создается очень важная информация, несколько поддельных цифровых репозиториев могут быть созданы параллельно с оригиналом, так что даже если один будет взломан, то не будет обеспечена уверенность относительно содержимого.

Настоящее изобретение позволяет сортировать, систематизировать и сертифицировать огромное количество информации, с которой приходится сталкиваться в настоящее время, с помощью быстрых и гибких протоколов, фильтрующих Большие Данные и преобразующих их во что-то более простое в управлении.

Не ограничивающие примеры реализуемых с помощью компьютера системы и способа в соответствии с предпочтительными вариантами осуществления изобретения приведены ниже.

Примеры

Пример 1.

В приведенном для примера варианте осуществления изобретения цифровая идентичность (104) первого пользователя (102-1) содержит средства (114) аутентификации отличительной метки, имеющие, помимо прочего, оптические свойства материала.

Указанная отличительная метка (114) выращена с получением монолитной структуры непосредственно на датчике КМОП (ASIC), который действует в качестве измерительного устройства.

При освещении светодиодами разных длин волн отличительная метка обеспечивает получение радужных цветов с различной отражательной способностью. Датчик КМОП считывает данные из отличительной метки, освещенной светом с различными длинами волн, и связывает измерения со значениями в альфа-таблице. Из отличительной метки случайным образом извлекается строка по меньшей мере в 10-20 значений, обеспечивая таким образом получение кода для аутентификации, который может быть подтвержден посредством сертификационного объекта.

Пример 2.

Транзакция (106) между двумя пользователями (102) предоставляется в сеть (101) для совместного использования данных через вычислительные устройства (103) указанных пользователей. Цифровая идентичность (104) двух пользователей верифицируется сертификационным объектом (105), сравнивающим коды для аутентификации, выработанные по отличительным меткам указанных двух пользователей, при этом код для аутентификации, обеспеченный соответствующими двойными отличительными метками, сохраненными сертификационным объектом, считывается таким же образом. При успешной аутентификации отличительных меток выдается электронный сертификат (113) в вычислительное устройство (103) каждого проверенного пользователя (102'), при этом транзакция является авторизованной и выполняется. После этого цифровая информация, относящаяся к транзакции, сохраняется по меньшей мере в одном цифровом репозитории (107), в то время как в базу (108) данных личного регистрационного учета каждого из двух проверенных пользователей (102') добавляется новый блок (118) с записью цифрового адреса указанного как минимум одного цифрового репозитория (107).

Таким образом создаются нейронные связи (109) между цифровым репозиторием (107) и базами (108) данных личного регистрационного учета двух пользователей.

Сохраненная цифровая информация транзакции доступна только указанным двум пользователям после проверки их цифровых идентичностей при каждом новом соединении с цифровым репозиторием (107).

Пример 3.

Отличительная метка пользователя и его двойная отличительная метка в соответствии с предпочтительными вариантами осуществления изобретения используются, как показано ниже, в способе шифрования информации, наподобие такого шифрования, для которого используются шифровальные книги. Отличительная метка пользователя опрашивается для аутентификации посредством ее освещения с пер-

вой длиной w1 волны в данной точке отличительной метки с координатами x, y. Интенсивность света, испускаемого отличительной меткой в указанном положении, измеряют измерительным устройством и получают значение (x, y, I1); посредством связывания с указанным значением буквенно-цифрового символа шифруют сообщение (x, y, #). Используют вторую длину w2 волны для освещения той же отличительной метки в том же положении и измеряют (x, y, I2) второе значение интенсивности света с получением кода (x, y, I2) для аутентификации. Код для аутентификации передают в процессор репозитория аппаратного типа, хранящего двойную отличительную метку. Используют длину w2 волны для освещения двойной отличительной метки в одном и том же (x, y) местоположении с аутентификацией, т.е. проверки подлинности, кода (x, y, I2) для аутентификации, затем используют первую длину w1 волны для освещения двойной отличительной метки в точке (x, y) положения с получением значения (x, y, I1) и расшифровкой сообщения (x, y, #).

Аналогичный эффект может быть получен посредством освещения на одной длине волны двух отличительных меток в одном и том же положении, изменяя при этом свойства их материалов посредством внешних воздействий (т.е. электрическим полем для оптоэлектрических материалов).

Аналогичный эффект также может быть получен посредством применения воздействий (электрических, магнитных и т.д.) в различных условиях для получения другой реакции от отличительной метки.

Пример 4.

На фиг. 7 показан следующий рабочий пример.

Осуществляется первая продажа (транзакция), в которую вовлечены следующие пользователи: продающая сторона, покупающая сторона, поставщик/дистрибьютор и правительство (последнее для уплаты НДС с продажи). При необходимости сам объект транзакции также может быть вовлечен в качестве пользователя при условии, что он владеет своей цифровой идентичностью.

Между всеми пользователями устанавливается смарт-контракт.

Создается цифровой репозиторий (107-1), в котором хранится вся информация (106-1), относящаяся к продаже. Доступ к данным (для считывания, изменения и т.д.) предоставляется в соответствии с правами, по которым достигнута договоренность между пользователями. Продающей стороне необходимо принять внутри две разные информации, поэтому продающей стороне предоставляется двойное право. Для каждого права создается новый блок в книгах личного регистрационного учета пользователей (соответственно: 108-1 для продающей стороны, 108-2 для покупающей стороны, 108-3 для поставщика и 108-4 для правительства) согласно смарт-контракту.

В случае продающей стороны, данной стороне необходимо добавить блок как в свою личную книгу (108-1a) бухгалтерского учета, так и в конкретную личную книгу (108-1b) управленческого учета, где хранится информация для сбора статистики и ускорения принятия управленческих решений на основе доступной информации. Блок также добавляется для покупающей стороны, поставщика и личных книг бухгалтерского учета НДС.

Посредством протокола аутентификации отличительных меток пользователей, вовлеченных в транзакцию, создается зашифрованная связь между репозиториями (107-1) и блоками различных баз данных личного регистрационного учета. Когда продающая сторона совершает другую продажу (транзакцию 106-2), тот же процесс воспроизводится с новыми пользователями, вовлеченными в эту новую транзакцию. Для продающей стороны это приводит к добавлению нового блока в предыдущие базы (108-1a и 1b) данных личного регистрационного учета или в другие, если в смарт-контракте указано иное. Блоки различных баз данных личного регистрационного учета обеспечивают регистрационный учет всех зарегистрированных транзакций и связь-ссылку, которая может быть активирована посредством последующей аутентификации отличительной метки для различных транзакций.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Реализуемая с помощью компьютера система (100) для безопасных хранения и передачи цифровых данных между пользователями (102) сети (101) для совместного использования данных, содержащая:

(a) множество вычислительных устройств (103) пользователей для доступа к сети (101) для совместного использования данных;

(b) цифровую идентичность (104), связанную с каждым пользователем (102) сети (101) и содержащую средства (114) аутентификации, при этом указанные средства (114) аутентификации содержат процессор, выполненный с возможностью автоматической выработки кода для аутентификации в ответ на запрос для проверки цифровой идентичности (104) пользователя (102), причем обеспечена возможность выработки нового кода для аутентификации в ответ на каждый новый запрос;

(c) по меньшей мере один сертификационный объект (105), сообщающийся со средствами (114) аутентификации и вычислительными устройствами (103) системы (100) и содержащий процессор, выполненный с возможностью проверки цифровой идентичности (104) пользователя посредством выдачи запроса в средства (114) аутентификации и проверки кода для аутентификации, выработанного средствами аутентификации в ответ на запрос, и выполненный с возможностью выдачи электронного сертификата

(113) для вычислительных устройств (103) проверенных пользователей (102'), цифровая идентичность (104) которых проверена;

(d) по меньшей мере одну транзакцию (106), в которую вовлечены два или более пользователей (102), авторизованную посредством проверки цифровых идентичностей (104) указанных двух или более пользователей посредством указанного по меньшей мере одного сертификационного объекта (105), при этом каждая транзакция (106) содержит цифровую информацию, которая выработана по меньшей мере одним из указанных двух или более проверенных пользователей (102'), принадлежит ему и/или находится в совместном использовании;

(e) по меньшей мере один цифровой репозиторий (107), имеющий цифровой адрес и хранящий по меньшей мере часть цифровой информации авторизованной транзакции (106), при этом указанный цифровой репозиторий (107) содержит шлюз, выполненный с возможностью обеспечения совместного использования цифровой информации только вычислительными устройствами (103) одного или более проверенных пользователей (102'), вовлеченных в транзакцию (106);

(f) базу (108) данных личного регистрационного учета, связанную с каждым пользователем (102) сети (101), хранящуюся в вычислительном устройстве (103) пользователей или сообщающуюся с вычислительным устройством (103) пользователей, при этом каждая база (108) данных личного регистрационного учета содержит блоки, связанные криптографическим ключом, и имеет такую структуру, что, когда авторизована транзакция (106) между двумя или более проверенными пользователями (102'), в базы (108) личных данных, связанные с каждым из указанных двух или более проверенных пользователей (102'), добавлен новый блок (118), причем в указанном новом блоке (118) записаны цифровые адреса по меньшей мере одного цифрового репозитория (107), хранящего по меньшей мере часть цифровой информации указанной транзакции (106).

2. Реализуемая с помощью компьютера система (100) по п.1, в которой средства (114) аутентификации цифровой идентичности (104) представляют собой отличительную метку, содержащую множество точек, имеющих одно или более измеримых свойств материала, при этом отличительная метка дополнительно содержит процессор, выполненный с возможностью выработки кодов для аутентификации посредством шифрования значений, полученных путем случайного измерения по меньшей мере одного из указанного измеримых свойств материала в различных точках отличительной метки посредством измерительного устройства, причем предпочтительно отличительная метка (114) либо выполнена в виде однокристальной системы, пакетированной с измерительным устройством, либо она выращена с получением монолитной структуры на измерительном устройстве, выполненном с возможностью измерения указанного по меньшей мере одного измеримого свойства материала, при этом предпочтительно указанное по меньшей мере одно из измеримых свойств материала отличительной метки (114) является физическим и/или химическим свойствами; более предпочтительно оптическим, электрическим, топографическим, механическим, тепловым, магнитным, химическим свойствами и комбинациями указанного.

3. Реализуемая с помощью компьютера система (100) по п.2, дополнительно содержащая по меньшей мере одну двойную отличительную метку, связанную с каждой отличительной меткой (114) и являющейся идентичной копией отличительной метки (114), причем двойная отличительная метка включает в себя процессор, выполненный с возможностью сообщения с отличительной меткой (114) и расшифровки кода для аутентификации, выработанного отличительной меткой (114); причем указанный по меньшей мере один сертификационный объект (105) представляет собой репозиторий аппаратного типа, сообщающийся с отличительными метками (114) и хранящий двойные отличительные метки, а также выполненный с возможностью исполнения протокола аутентификации для проверки цифровой идентичности (104) пользователя, который включает: запрос в отношении отличительной метки (114) пользователя (102) с получением кода для аутентификации, расшифровку указанного кода для аутентификации посредством двойной отличительной метки, подтверждение подлинности отличительной метки (114), проверку цифровой идентичности (104) пользователя, выдачу электронного сертификата (113) в вычислительное устройство (103) проверенного пользователя (102').

4. Реализуемая с помощью компьютера система (100) по любому из пп.2, 3, в которой отличительная метка дополнительно выполнена с возможностью шифрования и дешифрования информации, предпочтительно посредством протоколов математических алгоритмов, более предпочтительно посредством измерения по меньшей мере одного из указанного множества измеримых свойств материала в различных случайных точках, получения значений и преобразования посредством алгоритма строки полученных значений в криптографический код.

5. Реализуемая с помощью компьютера система (100) по любому из пп.1-4, в которой средства (114) аутентификации представляют собой тонкую пленку, причем указанная пленка предпочтительно имеет до 106 точек, имеющих различные измеримые свойства материала на квадратный миллиметр.

6. Реализуемая с помощью компьютера система (100) по любому из пп.1-5, в которой по меньшей мере один пользователь (102) сети (101) является объектом, содержащим вычислительное устройство (103), и/или в которой по меньшей мере один цифровой репозиторий (107) и/или по меньшей мере один сертификационный объект (105) также является пользователем (102) сети, имеющим свою цифровую идентичность (104).

7. Реализуемая с помощью компьютера система (100) по п.1, в которой по меньшей мере один цифровой репозиторий (107) или поставщик указанного по меньшей мере одного цифрового репозитория (107) также является сертификационным объектом (105).

8. Реализуемая с помощью компьютера система (100) по любому из пп.1-7, в которой цифровая информация, которая выработана по меньшей мере одним из указанных двух или более проверенных пользователей (102'), принадлежит ему и/или находится в совместном использовании, содержит смарт-контракт, определяющий обязанности и права указанных двух или более проверенных пользователей (102') в отношении указанной цифровой информации.

9. Реализуемая с помощью компьютера система (100) по любому из пп.1-8, в которой цифровая идентичность (104) пользователя (102) включает в себя публичное имя пользователя.

10. Реализуемая с помощью компьютера система (100) по любому из пп.1-9, в которой средства (114) аутентификации представляют собой маркер аппаратных средств или физически неклонируемую функцию (Physical Unclonable Function, PUF).

11. Реализуемая с помощью компьютера система (100) по любому из пп.1-10, дополнительно включающая в себя:

(g) одну или более боковых цепочек, прикрепленных к одной или более базам (108) данных личного регистрационного учета, связанным с пользователями (102) сети (101).

12. Реализуемая с помощью компьютера система (100) по любому из пп.1-11, в которой сеть для совместного использования данных является Интернетом, предпочтительно Интернетом вещей или Интернетом всего.

13. Реализуемый с помощью компьютера способ безопасных хранения и передачи цифровой информации между пользователями сети для совместного использования данных, выполняемый компьютерной системой (100) по п.1, включающий:

i) осуществление доступа по меньшей мере двух пользователей (102) к сети (101) для совместного использования данных посредством вычислительных устройств (103);

ii) предоставление транзакции (106) между указанными по меньшей мере двумя пользователями (102) сертификационному объекту (105), при этом указанная транзакция (106) содержит цифровую информацию;

c) аутентификацию цифровых идентичностей (104) указанных по меньшей мере двух пользователей (102) посредством указанного по меньшей мере одного сертификационного объекта (105) с получением по меньшей мере двух проверенных пользователей, цифровая идентичность (104) которых подтверждена;

d) выдачу электронного сертификата (113) проверенным пользователям (102');

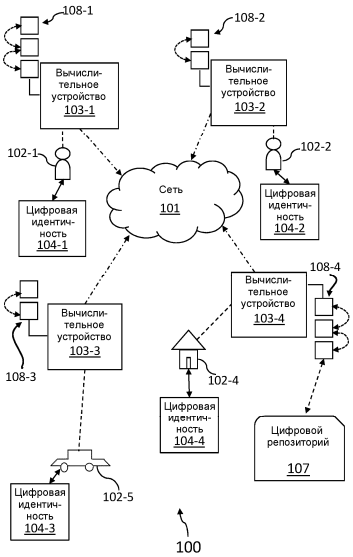
e) авторизацию транзакции (106);

f) сохранение цифровой информации авторизованной транзакции (106) по меньшей мере в одном цифровом репозитории (107), имеющем цифровой адрес;

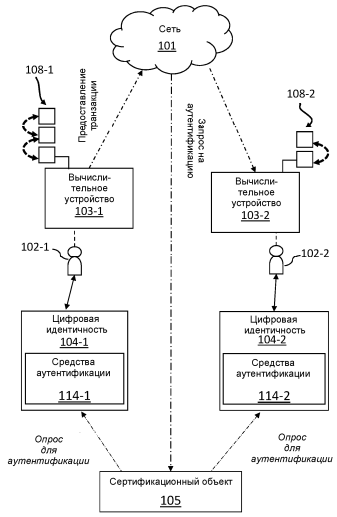
g) запись цифрового адреса указанного по меньшей мере одного цифрового репозитория (107), хранящего цифровую информацию транзакции, в новых блоках (118) баз (108) данных личного регистрационного учета, связанных с каждым из указанных проверенных пользователей (102').

14. Реализуемая с помощью компьютера система по любому из пп.1-12 или реализуемый с помощью компьютера способ по п.13, в которой или согласно которому цифровая информация не может быть изменена проверенными пользователями (102'), и/или в которой или согласно которому цифровая информация транзакции распространена в нескольких цифровых репозиториях.

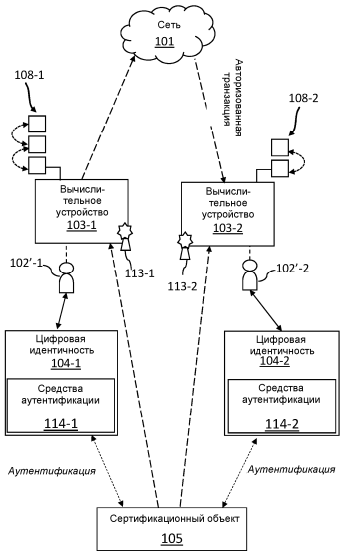
15. Реализуемая с помощью компьютера система по любому из пп.1-12 или реализуемый с помощью компьютера способ по любому из пп.13-14, в которой или согласно которому блоки базы (108) данных личного регистрационного учета семантически связаны между собой, содержат один и тот же хэштег, ключевое слово, одно и то же число или одну и ту же строку.



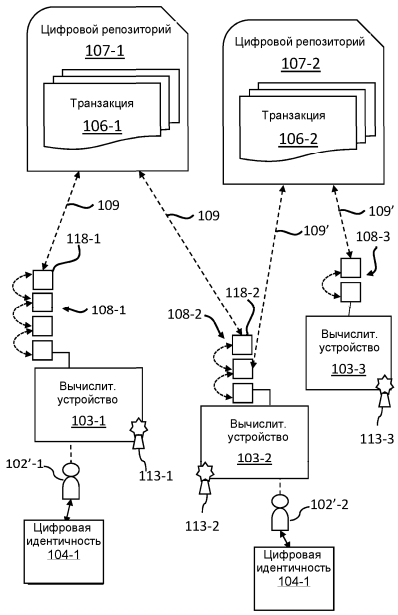
Фиг. 1



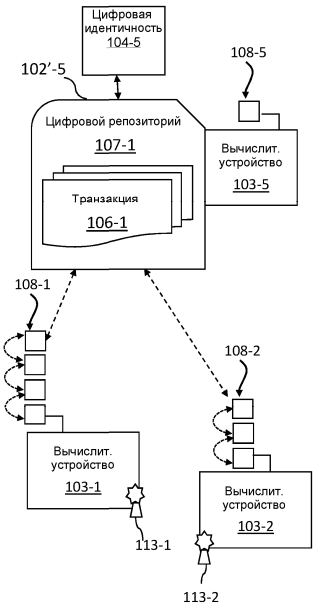
Фиг. 2A



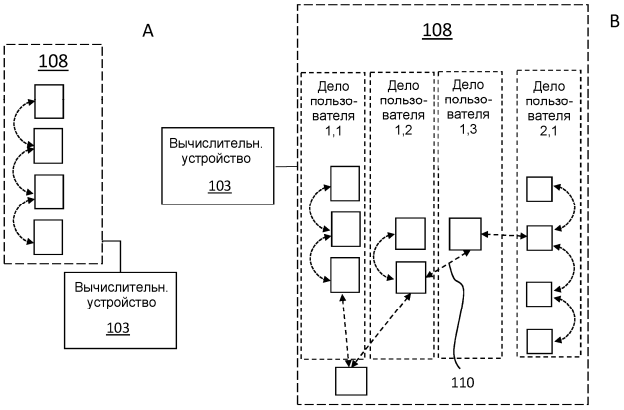
Фиг. 2B



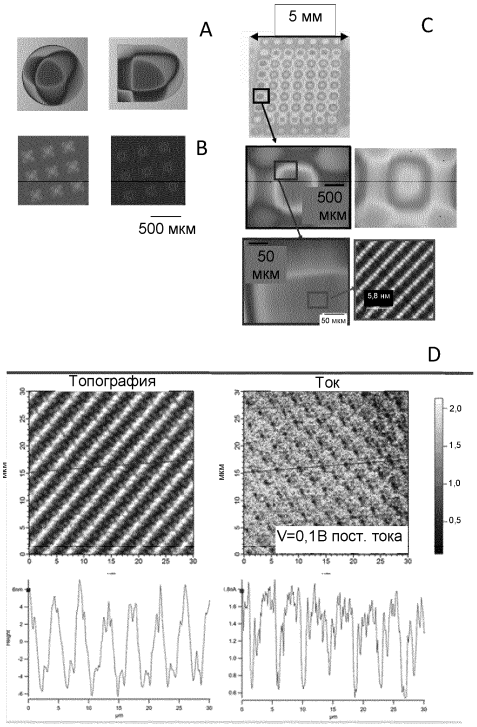
Фиг. 3



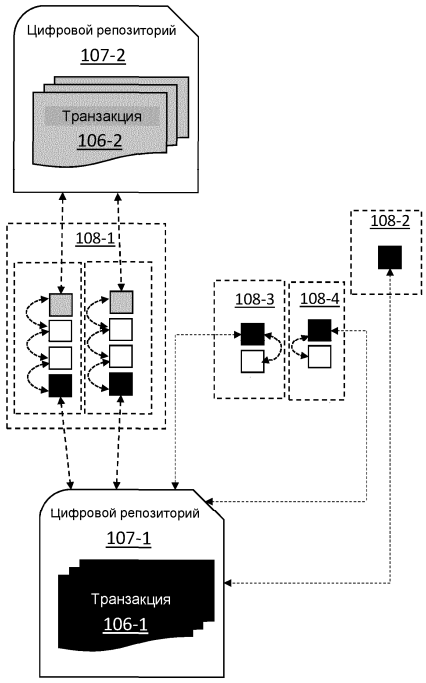
Фиг. 4



Фиг. 5


A
B
C
D
5 мм
500 мкм
500 мкм
50 мкм
Топография
Ток
V=0,1В пост. тока

Фиг. 6


Цифровой репозиторий
107-2
Транзакция
106-2
108-1
108-2
108-3
108-4
Цифровой репозиторий
107-1
Транзакция
106-1

Фиг. 7