РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2018 142 891** (13) **A**

(51) МПК
G06F 21/51 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2018142891, 01.06.2017**

Приоритет(ы):
(30) Конвенционный приоритет:
06.06.2016 US 62/346,431;
18.10.2016 US 15/296,953

(43) Дата публикации заявки: **05.06.2020** Бюл. № **16**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **05.12.2018**

(86) Заявка PCT:
US 2017/035341 (01.06.2017)

(87) Публикация заявки PCT:
WO 2017/213943 (14.12.2017)

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(71) Заявитель(и):
МАЙКРОСОФТ ТЕКНОЛОДЖИ ЛАЙСЕНСИНГ, ЭлЭлСи (US)

(72) Автор(ы):
ГРЭЙ, Джон Марли (US)

(54) КРИПТОГРАФИЧЕСКИЕ ПРИЛОЖЕНИЯ ДЛЯ БЛОКЧЕЙН-СИСТЕМЫ

(57) Формула изобретения

1. Компьютерная система для делегирования модели поведения, ассоциированной с контрактом, установленным по цепочке блоков, приложению не в цепочке блоков, при этом компьютерная система содержит:

один или более машиночитаемых носителей, хранящих машиноисполняемые инструкции криптоделегата и контейнерной службы криптлета, при этом

криптоделегат включает в себя инструкции, которые принимают из кода контракта, исполняющегося на виртуальной машине, идентификацию криптлета и запрошенную модель поведения, которая должна выполняться криптлетом, предоставляют контейнерной службе криптлета идентификацию и запрошенную модель поведения, принимают от контейнерной службы криптлета ответ, сформированный криптлетом, выполняющим запрошенную модель поведения, и отправляют коду контракта ответ; и

контейнерная служба криптлета включает в себя инструкции, которые сохраняют информацию, относящуюся к зарегистрированным криптлетам, включающую в себя ссылки на криптлеты, принимают от криптоделегата идентификацию и запрошенную модель поведения, идентифицируют хост для исполнения контейнера криптлета и криптлета, аутентифицируют криптлет, предоставляют запрошенную модель поведения криптлету, принимают ответ, сформированный криптлетом, и отправляют этот ответ

RU 2018142891 A

RU 2018142891 A

цепочке блоков и проверяют его посредством криптоделегата; и

один или более процессоров для исполнения машиноисполняемых инструкций, хранящихся на одном или более машиночитаемых носителей.

2. Компьютерная система по п.1, в которой криптоделегат исполняется посредством виртуальной машины.

3. Компьютерная система по п.1, в которой запрошенная модель поведения должна отправлять события контракту.

4. Компьютерная система по п.1, в которой криптоделегат дополнительно включает в себя инструкции, чтобы принимать код криптлета от контракта и предоставлять код контейнерной службе криптлета, при этом контейнерная служба криптлета проверяет код, формируя хеш кода и проверяя, что он соответствует хешу, предоставленному контрактом, записывает код в цепочке блоков регистрации криптлета и инструктирует аттестованному хосту исполнять криптлет для выполнения запрошенной модели поведения.

5. Компьютерная система по п.1, в которой криптоделегат записывает в цепочке блоков, ассоциированной с контрактом, указание каждого запроса и ответа, предоставляемого контракту.

6. Компьютерная система по п.1, в которой контракт предоставляет криптоделегату указание хоста, который должен исполнять криптлет.

7. Способ, выполняемый посредством вычислительной системы, при этом способ содержит этапы, на которых:

принимают от смарт-контракта, исполняемого посредством виртуальной машины, запрос на регистрацию контрактного криптлета для выполнения модели поведения от имени смарт-контракта, код контрактного криптлета и указание аттестованного хоста, чтобы исполнять код контрактного криптлета;

проверяют код контрактного криптлета;

сохраняют код контрактного криптлета в цепочке блоков контрактного криптлета и хранилище данных;

принимают от смарт-контракта запрос для контрактного криптлета, чтобы выполнять модель поведения;

инструктируют контрактному криптлету исполняться на аттестованном хосте; и

отправляют контрактному криптлету, исполняющемуся на аттестованном хосте, запрос на выполнение модели поведения;

при этом обмены данными со смарт-контрактом и контрактным криптлетом происходят по защищенным каналам.

8. Способ по п.7, в котором проверка кода включает в себя этапы, на которых формируют хеш кода и сравнивают хеш с общедоступным ключом, ассоциированным с кодом.

9. Способ по п.7, в котором запрос, который принимается от смарт-контракта, принимается через криптоделегата, который исполняется посредством виртуальной машины.

10. Способ по п.9, в котором криптоделегат записывает в цепочке блоков смарт-контракта указание обмена данными со смарт-контрактом и криптоделегатом.

11. Способ по п.7, в котором виртуальная машина исполняется на узле цепочки блоков, а аттестованный хост является компьютером, который является внешним по отношению к узлам цепочки блоков.

12. Способ по п.7, в котором цепочка блоков регистрации криптлета является отдельной от цепочки блоков смарт-контракта.

13. Способ, выполняемый посредством одной или более вычислительных систем, при этом способ содержит этапы, на которых:

RU 2018142891 A

RU 2018142891 A

инструктируют исполнение посредством виртуальной машины смарт-контракта, ассоциированного с цепочкой блоков;

во время исполнения смарт-контракта отправляют через криптоделегата контейнерной службе криптлета запрос на делегирование модели поведения криптлету, который исполняется на аттестованном хосте; и

во время исполнения контейнерной службы криптлета

идентифицируют хост для исполнения кода криптлета;

инструктируют идентифицированному хосту исполнять код криптлета для выполнения делегированной модели поведения;

принимают от криптлета ответ на запрошенную модель поведения; и

отправляют ответ смарт-контракту по цепочке блоков, признанной действительной криптоделегатом.

14. Способ по п.13, в котором криптоделегат устанавливает защищенный канал связи с контейнерной службой криптлета, и контейнерная служба криптлета устанавливает защищенный канал связи с хостом.

15. Способ по п.13, в котором криптлет является контрактным криптлетом, код криптлета предоставляется или идентифицируется посредством смарт-контракта, и хост идентифицируется посредством смарт-контракта.

RU 2018142891 A

RU 2018142891 A