УДК 338:681.3

СФЕРЫ ПРИМЕНЕНИЯ СМАРТ-КОНТРАКТОВ И РИСКИ ПРИ РАБОТЕ С НИМИ

© **Кардонов А. В., 2018**
Иркутский государственный университет, г. Иркутск

В статье дается определение смарт-контракта, описываются основные сферы его применения ипривводятся процессы, подобные смарт-контрактам, но работающие вне блокчейн. Также рассмотрены некоторые риски, возникающие при работе со смарт-контрактами.

Ключевые слова: блокчейн, криптовалюта, смарт-контракт, риск-менеджмент

Для лучшего понимания, введем два термина. Смарт-контракт — это автоматически исполняющийся процесс, в котором предусмотрены все возможные варианты развития событий и отсутствует возможность внесения изменений. Обязательным условием существования смарт-контракта является наличие среды исполнения [1].

В настоящее время смарт-контракты реализуются в разнообразных блокчейн системах, среди которых одной из самых известных является система Ethereum, разработанная специально для обеспечения их функционирования.

Оракул — это программа, существующая вне блокчейн системы и поставляющая в нее данные. Оракул может использовать в качестве входных данных как физические данные [2], так и цифровые.

Рассмотрим несколько сфер применения смарт-контрактов.

Торговля. Практически все виды существующих взаимоотношений при товарно-денежном обмене могут быть реализованы в виде контрактов. В литературе довольно часто можно найти описание алгоритма действия смарт-контрактов при торговле самыми разными видами товара, начиная от продажи автомобилей и заканчивая продажей недвижимости. Привлекательностью смарт-контрактов является заложенная в его суть возможность определения и закрепления в неизменном виде условий сделки участников, не доверяющих друг другу.

Классическим прототипом смарт-контракта является сервис защиты покупателя на Aliexpress (и не только на этой торговой площадке) — escrow служба. При оплате товара сумма сразу списывается с покупателями, но продавец не получает этих денег до тех пор, пока не выполнится одно из двух условий, либо покупатель подтвердит получение товара, либо с момента проведения сделки пройдет определенное время. После выполнения любого из этих условий произойдет автоматическое перечисление средств на счет продавца. Существуют и условия внутри смарт-контракта:

- продление защиты покупателя — в этом случае срок ожидания подтверждения получения товара увеличивается на какое-то время;
- сообщение покупателя о нарушении условий сделки (неполучение товара, товар не соответствует описанию или ненадлежащего качества) — в этом случае автоматическая работа смарт-контракта прерывается и сотрудниками Aliexpress (квази Оракулом) осуществляется рассмотрение сути претензии и вынесение решения, после чего это решение вновь становится входной информацией

для смарт-контракта для возврата денег (части денег) или их перечисления(возможно частичного) на счет продавца.

В качестве еще одного, простейшего примера прототипа смарт-контракта в сфере торговли, можно назвать автоплатеж для пополнения баланса сотового телефона.

Смарт-контракты вполне серьезно рассматриваются как альтернатива существующим биржам для проведения сделок с ценными бумагами. Учитывая тот факт, что ценные бумаги в настоящее время практически все виртуализированы и существуют только в виде электронных реестров, перевод торговли ценными бумагами в блокчейн лишь вопрос времени.

В качестве примера приведу проведенную 29 сентября 2017 года первую в России сделку с ценными бумагами с использованием смарт-контрактов в блокчейн. Данная сделка была проведена «Национальным расчетным депозитарием» и состояла из выполнения поручения Райффайзенбанка на покупку облигаций Мегафона [3]. Более подробно технические аспекты проведения сделки описаны сотрудником Раффайзенбанка, участвовавшим в ее организации [4].

Если обратиться к сфере медицинских услуг, то можно увидеть что, для уже достаточно давно вынашиваемой идеи размещать истории болезней в облачных ресурсах, блокчейн является прекрасным вариантом реализации. При этом область применения смарт-контрактов поистине безгранична. Например, они могут автоматически обрабатывать поступающие результаты анализов пациента и на основании этого делать вывод о необходимости посещения врача. И даже осуществлять самостоятельную запись пациента к необходимому специалисту. При наличии оракулов, реализованных в виде персональных датчиков, смарт-контракты могут в режиме реального времени анализировать состояние здоровья пациента и предлагать ему разнообразные модели поведения для улучшения состояния.

Простейший пример — получающие все большее распространение, «умные» часы, считающие количество шагов, пройденных за день, ведущие мониторинг пульса в течение дня, фиксирующие качество и количество сна в сутки, а также многое другое и передающие эти данные в сеть, где уже сейчас можно посмотреть всю историю фиксируемых событий.

При этом в качестве контрагентов данных смарт-контрактов будут выступать организации, представляющие сервис и пользователи этих сервисов.

Менеджмент. В этой сфере смарт-контракты вполне могут использоваться как элементы организации деятельности, как организаций, так и персоналий. Так как практически все виды деятельности, как правило, цикличны — не представляет особого труда выявить цепочки задач и автоматизировать инициализацию следующей задачи сразу по окончанию предыдущей.

На основании смарт-контрактов можно построить ERP систему, систему HelpDesk и тому подобные системы, процессы которых в большинстве своем уже формализованы и описаны с помощью ITIL, COBIT, ISO20000, а также иных стандартов и библиотек.

В качестве прототипа смарт-контракта из жизни вполне можно рассматривать формализованные бизнес-процессы предприятий. Будучи единожды описанные, они начинают свое самостоятельное функционирование по заданному алгоритму.

Также интересной сферой для приложения свойств смарт-контрактов является социология. Сбор разнообразными Оракулами всех данных (по сути, мы говорим о BigData) из сети интернет и их обработка на постоянной основе смарт-контрактами позволит описывать и формализовать все доступные объекты.

Ярким примером ведущихся в этом направлении разработок является система социального рейтинга в Китайской народной республике. Результат разработки и внедрения такой системы полностью перевернет основы социальных взаимоотношений в этом государстве.

Вкратце коснусь достаточно специфической сферы применения смарт-контрактов — обеспечение краудсорсинга в блокчейн. В этом случае при помощи смарт-контрактов проводится ICO(Initial Coin Offering — первичное размещение средств) и выпускаются токены для участников.

Однако, несмотря на всю свою мощь и привлекательность, смарт-контракты являются источником рисков. Рассмотрим некоторые виды рисков.

Риск № 1. Ошибки при разработке смарт-контрактов.

Правила написания смарт-контрактов на текущий момент не формализованы, но главное — не описаны правила их верифицирования. При этом нет возможности внести в смарт-контракт изменения, так как он по определению неизменяем.

Простейший пример: заключается смарт-контракт, по условиям которого покупатель резервирует сумму для перевода денег при поступлении на склад товара. Но программный код смарт-контракта был написан с ошибкой — не была реализована процедура проверки поступления товара на склад. В результате деньги покупателем уплачены, но к продавцу никогда не попадут, вне зависимости от того поставил он товар или не поставил. Деньги для продавца потеряны.

Особенно тщательно должны разрабатываться и тестироваться смарт-контракты при ICO [5].

Риск № 2. Компрометация Оракулов.

Напомню, что программы Оракулы — это специализированные сервисы, призванные обеспечить привязку цифрового мира к реальному и предоставить смарт-контрактам входные данные для их исполнения.

Возникает вопрос неизменности и достоверности полученных данных от этих сервисов.

Например, злоумышленник может атаковать Оракул, выдающий данные о курсе обмена валют для контрактов, занимающихся обменом валют. После изменения его кода он будет выдавать неверные данные, что влечет за собой вполне конкретные финансовые риски для смарт-контрактов, использующих эти данные.

Также можно подменять информацию, либо модифицировать физическую информацию, поступающую на вход Оракулу. Простейший пример — накрыть светонепроницаемым предметом датчик Оракула передающего в смарт-контракт «Умного города» информацию об освещенности. В этом случае Оракул будет постоянно считать, что темно и,вследствие этого смарт-контракт не будет гасить уличные фонари.

Риск № 3. Утеря доступа.

Вся работа с блокчейн построена на том факте, что авторизовать себя в системе можно только с использованием закрытой части криптографического ключа.

Если в случае обычных контрактов, сделок и т.д. существует возможность авторизоваться с помощью третьих сторон (суд, органы, выдающие документы, нотариат, рекомендации т и т.д.), то в случае блокчейн и смарт-контрактов такая возможность не предусмотрена. Если закрытая часть ключа потеряна, вы никогда не сможете ее восстановить.

Риск № 4. Отсутствие правового поля.

Невыполнение обычного контракта в реальном мире может являться предметом судебного разбирательства. Мир блокчейн в настоящее время не является объектом правового поля. Все сделки, проводимые в рамках смарт-контрактов, обеспечиваются только доброй волей участников.

Риск № 5. Отсутствие возможности страхования рисков.

В связи с тем, что на текущий момент правовое поле при работе с блокчейн не определено, страхование рисков на этом рынке отсутствует. При возникновении любых риск-событий со смарт-контрактом все финансовые последствия целиком ложатся только на его участников.

В заключение считаю необходимым выдвинуть, может быть неожиданное, но, на мой взгляд, интересное предположение как о смарт-контрактах, так и о блокчейн в целом:

Блокчейн-системы, как и смарт-контракты хороши для обеспечения взаимодействия субъектов без использования посредников, но срок их жизни ограничен появлением искусственного интеллекта. После появления на свет развитого, лишенного чувств и заинтересованности искусственного интеллекта, место в качестве арбитра и доверенного лица будет занято им. Соответственно исчезнет необходимость в децентрализованных системах, основанных на подтвержденных консенсусах. ■

1. Alyoshkin R. О смарт-контрактах простыми словами // Хабрахабр. 15.09.2017. – [Электронный ресурс]. – URL:https://habrahabr.ru/company/kaspersky/blog/337984/ (Дата обращения: 20.11.2017).

2. Karionov E. Понимание оракулов в блокчейне (перевод статьи ThomasBertani из блога компании Oraclize). // Хабрахабр. 09.07.2017. – [Электронный ресурс]. – URL: https://habrahabr.ru/post/332678/ (Дата обращения: 25.11.2017)

3. Пресс релиз Национального расчетного депозитария. 02.10.2017. – [Электронный ресурс]. – URL:https://www.nsd.ru/ru/press/pressrel/index.php?id36=633628 (Дата обращения: 27.11.2017).

4. Павел Mad Jackal. Мегафон-Райффайзенбанк — первая в России сделка по ценным бумагам на блокчейне. // Хабрахабр. 14.11.2017. – [Электронный ресурс]. – URL: https://habrahabr.ru/company/raiffeisenbank/blog/341850/ (Дата обращения: 27.11.2017)

5. Прилуцкий С. Технические особенности проведения ICO. Начало. // Хабрахабр. 10.11.2017. – [Электронный ресурс]. – URL:https://habrahabr.ru/post/342102/ (Дата обращения: 27.11.2017)

СПИСОК ЛИТЕРАТУРЫ

Alyoshkin R. О смарт-контрактах простыми словами // Хабрахабр. 15.09.2017. – [Электронный ресурс]. – URL:https://habrahabr.ru/company/kaspersky/blog/337984/ (Дата обращения: 20.11.2017).

Karionov E. Понимание оракулов в блокчейне (перевод статьи ThomasBertani из блога компании Oraclize). // Хабрахабр. 09.07.2017. – [Электронный ресурс]. – URL: https://habrahabr.ru/post/332678/ (Дата обращения: 25.11.2017)

Пресс релиз Национального расчетного депозитария. 02.10.2017. – [Электронный ресурс]. – URL:https://www.nsd.ru/ru/press/pressrel/index.php?id36=633628 (Дата обращения: 27.11.2017).

Павел Mad Jackal. Мегафон-Райффайзенбанк — первая в России сделка по ценным бумагам на блокчейне. // Хабрахабр. 14.11.2017. – [Электронный ресурс]. – URL: https://habrahabr.ru/company/raiffeisenbank/blog/341850/ (Дата обращения: 27.11.2017)

Прилуцкий С. Технические особенности проведения ICO. Начало. // Хабрахабр. 10.11.2017. – [Электронный ресурс]. – URL:https://habrahabr.ru/post/342102/ (Дата обращения: 27.11.2017)

Scopes of application of smart contracts and risks at work with them

The article describes the definition of a smart contract that describes the main areas of its application and describes processes that are similar to smart contracts, but operate outside the block system. Also considered are some of the risks that arise when working with smart contracts.

Keywords: block, crypto currency, smart contract, risk management