SMART-CONTRACTS

Dubitskaya E.G. (Russian Federation) Email: Dubitskaya339@scientifictext.ru

Dubitskaya Elena Grigorievna – Bachelor,
DIRECTION OF TRAINING: MATHEMATICS AND INFORMATION SYSTEMS ADMINISTRATION,
Graduate Student,
DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGIES,
SAINT-PETERSBURG MINING UNIVERSITY, SAINT-PETERSBURG

Abstract: *in the modern world every day there are a variety of technologies. Most of the society does not have a proper idea of what blockchain technology and related technologies are. This article will discuss one of these technologies — smart contracts. The reader will be disclosed the key concepts of smart contracts, their types, differences between smart contracts from the usual, as well as the basic principles of smart contracts. After reading this article will be a General idea of these technologies of the 21st century.*
Keywords: *smart contract, blockchain.*

СМАРТ-КОНТРАКТЫ

Дубицкая Е.Г. (Российская Федерация)

Дубицкая Елена Григорьевна – бакалавр,
направление подготовки: математическое обеспечение и администрирование информационных систем,
магистрант,
кафедра информационных систем и технологий,
Санкт-Петербургский горный университет, г. Санкт-Петербург

Аннотация: *в современном мире каждый день появляются различные технологии. Большая часть общества не имеет должного представления о том, что такое технология блокчейн и связанные с ней технологии. В данной статье будет рассмотрена одна из таких технологий — смарт-контракты. Читателю будут раскрыты ключевые понятия смарт-контрактов, их виды, отличия умных контрактов от обычных, а также основные принципы работы смарт-контрактов. После прочтения данной статьи появится общее представление о данных технологиях 21-го века.*
Ключевые слова: *смарт-контракт, блокчейн, умный контракт.*

Резкое развитие криптовалютного рынка в последние годы, несомненно, провоцирует специалистов углубляться в разработку инструментов для управления данным новшеством.

Использование блокчейн технологии расширяет представление о возможностях человечества. Благодаря данной технологии возможно создание смарт-контрактов - компьютерных алгоритмов, предназначенных для заключения и поддержания самоисполняемых контрактов, выполняемых в блокчейн-среде.

Блокчейн (от английского block chain, «цепочка блоков») – это распределённая база данных, доступ к которой может получить любой человек. Иначе её называют «технологией распределённого реестра», так как не существует какого-либо централизованного органа или регулятора, который мог бы распоряжаться блокчейном по собственному усмотрению.

Такие контракты записываются в виде кода, существующего в распределенном реестре — блокчейне, который поддерживается и управляется сетью компьютеров. Их назначение – передача информации и обеспечение исполнения условий контракта обеими сторонами. Иначе говоря, умные контракты позволяют обмениваться активами, не прибегая к услугам посредников.

Идея умных контрактов в современном мире представляет собой многообещающую облачную технологию.

Что такое смарт-контракт?

Смарт-контракт (или умный контракт) — это специальный протокол, предназначенный для сторон, которые могут участвовать в переговорах, проверять их условия, реализовывать договоренности и контролировать выполнение контракта. Это позволяет совершать надежные, отслеживаемые и необратимые транзакции без участия третьих сторон. В смарт-контракте содержится вся информация об условиях договора, а все предусмотренные контрактом действия выполняются автоматически.

В чем преимущества смарт-контактов?

1. Смарт-контракты дают возможность безопасно обмениваться деньгами, акциями, собственностью и другими активами напрямую, без участия внешних посредников в лице банков или государственных органов. Кроме того, такие транзакции являются прослеживаемыми, прозрачными и необратимыми.

2. Смарт-контракт зашифрован и хранится распределено, что гарантирует защиту от потери или несанкционированного изменения.

3. Смарт-контракты автоматически обеспечивают выполнение всех условий договора. Большая часть процесса автоматизирована, что позволяет сэкономить средства и время.

4. Умные контракты обеспечивают более быстрое разрешение вопросов. Как только условия контракта выполнены, стороны сразу же обмениваются активами.

5. Все транзакции в умных конрактах являются прослеживаемыми, прозрачными и необратимыми.

Для того чтобы заключить любую сделку, необходимо обратиться к нотариусу или адвокату, оплатить документы и ждать их оформления. Зачастую, многие пункты этих документов содержат ссылки на законодательные статьи, которые можно интерпретировать под себя, обойти. В случае невыполнения условий сделки, в реальной жизни людям приходится обращаться в суд, снова тратить деньги на процесс и доказывать свою правоту. При заключении таких сделок сомнительно наличие взаимного доверия участников договора. Данные факторы полностью исключаются в смарт-контрактах.

В чем слабые стороны смарт-контрактов?

Человеческий фактор. Пока что код смарт-контракта пишут люди, а не искусственный интеллект. Так как, смарт-контракт записывается в блокчейн, он не может быть в дальнейшем изменен.

Неопределенный правовой статус. Смарт-контракты являются абсолютно уникальным явлением. Потому пока многие государства не определили правовой статус смарт-контрактов. Данный фактор представляет собой определенные риски в будущем.

Защита устройства пользователя. Устройство может быть утеряно или запись с ключами, что лишит доступа в систему.

Отсутствие гибкости. Данный фактор дает и негативный эффект. Действия в смарт-контрактах прописаны однозначно. Если установлены определенные штрафы за нарушения, они будут исполнены в любом случае, независимо от того, как хорошо человек умеет договариваться с людьми в реальной жизни.

Суд. Если возникнет необходимость рассмотрения смарт-контракта в суде, то будет проблематично установить, когда был оформлен договор и был ли оформлен вообще. Нарушены ли были обязательства или нет. Надзор понадобится для разрешения спорных вопросов. А для интерпретации кода смарт-контракта потребуются невероятные навыки регулятора.

Таблица 1. Сравнение смарт-контрактов и обычных контрактов

Умный контракт	**Обычный контракт**
Это программа или транзакционный протокол, который использует в своей работе блокчейн	Бумажная версия документов
Основывается на коде	Основывается на праве и законодательных актах
Пишется на компьютерном языке	Пишется юридическим языком
Условия контракта невозможно изменить	Условия контракта можно изменить, переписать или интерпретировать по-другому
Условия контракта выполняются автоматически всеми участниками процесса	Условия контракта могут быть не выполнены или выполнены некачественно
При нарушении условий контракта автоматически происходит наказание, штраф или санкция, прописанные в контракте	При нарушении условий контракта необходимо обращаться в суд
Все сделки осуществляются без третьих лиц и посредников	Сделки осуществляются с множеством посредников. Необходимы помощь нотариуса, юриста и обращения в государственные службы
Транзакции проводятся с помощью криптовалют	Транзакции проводятся валютой через банки
При выполнении условий контракта, обмен	Обмен ценностями происходит с задержками

ценностями происходит мгновенно	
Все данные о контрагентах хранятся в блокчейне, и человек сам устанавливает, какая информация будет общедоступной	Информацию о контрагентах можно узнать лишь при условии, что он предоставит выписки и справки из государственных органов
Контракт можно заключить с человеком из любой точки мира без личного присутствия	Контракт подписывается лишь при личной встрече двух сторон или их доверенных лиц
Гарантируется безопасность сделки	Нет никаких гарантий. Любой закон можно обойти
При заключении контракта строго все условия соблюдаются в точности, в противном случае налаживается штраф или возврат денег покупателю	Условия можно изменить, договориться
Жульничество и мошенничество исключены	Вероятность обмана, подкупа, взяточничества очень высока
Для составления контракта необходима помощь программистов	Для составления контракта необходима помощь юристов

Первые смарт-контракты

Первые идеи смарт-контрактов были предложены в 1994 году Ником Сабо. Он описал смарт-контракт как компьютерный протокол, который на основе математических алгоритмов самостоятельно проводит сделки с полным контролем над их выполнением.

Впервые идеи Сабо воплотились на практике вместе с появлением первой криптовалюты биткоин и лежащей в ее основе технологии блокчейн. Некоторые принципы смарт-контрактов были заложены в протоколе биткоина. Однако большинство современных блокчейнов, включая биткоин, не обладают полнотой по Тьюрингу, поэтому их контракты представляют собой относительно простые конструкции, такие как мультиподпись или транзакции с отложенным исполнением.

Широкое практическое применение смарт-контракты получили с появлением и развитием проекта Ethereum. В 2013 году будущий его основатель Виталик Бутерин пришел к выводу, что биткоин плохо подходит в качестве базового протокола для смарт-контрактов, поскольку изначально не был спроектирован под эту задачу [1].

Как работает смарт-контракт?

Смарт-контракт записывается в блокчейн, где вся его логика помещается в программный контейнер — блок. Последний объединяет все сообщения, относящиеся к конкретному смарт-контракту. Сообщения могут выполнять роль входов и выходов программного кода смарт-контракта и приводить к каким-либо действиям за пределами блокчейна, в реальном или цифровом мире.

Необходимые составляющие смарт-контракта:

- **Предмет договора.** Необходим сам предмет договора и наличие необходимых для его исполнения инструментов (криптовалютных расчетных счетов, программ-оракулов и т. д.). Контракт должен иметь доступ к описываемым услугам или товарам. Также договор должен иметь возможность открыть и закрыть доступ к данному элементу.

- **Цифровые подписи.** Контракт использует методы электронной подписи на основе публичных и приватных ключей, имеющихся у двух или более сторон соглашения. Все участники инициируют соглашение, подписывая договор своими секретными ключами.

- Секретный ключ - Строка символов, открывающая доступ к токенам в определенном кошельке. Секретный ключ действует как пароль и известен только владельцу адреса.

- **Условия договора.** Условия смарт-контракта в форме точной последовательности операций, которые все участники договора подтверждают подписью, а также достоверность источника цифровых данных.

- **Децентрализованная платформа.** Наличие приватной децентрализованной среды (например, Ethereum), которая поддерживает входы и выходы для оракулов, обеспечивающих связь реального и цифрового мира. Контракт записывается в блокчейн этой платформы и распределенно хранится на ее узлах.

Какие бывают смарт-контракты?

В зависимости от степени автоматизации смарт-контракты могут быть:

1. Полностью автоматизированными.
2. С копией на бумажном носителе.
3. Преимущественно на бумажном носителе, при этом часть положений перенесена в программный код (например, когда автоматизированы только платежи).

Решения на базе блокчейна находятся лишь на ранней стадии развития. Технологии тестируются и дорабатываются. На сегодняшний день подавляющее большинство смарт-контрактов относятся к третьему типу, где автоматизированы лишь отдельные аспекты соглашений, в частности, обмен денежных средств на имущественные права.

Пример: покупка с использованием смарт-контракта квартиры через децентрализованный сервис продажи (оплата проводилась в Ethereum, а продавец территориально находился в Нью-Йорке).

Где еще могут использоваться смарт-контракты?

Потенциальные возможности и сферы использования смарт-контрактов обширны — от простой мультиподписи до операций с производными финансовыми инструментами. Мультиподпись (multisig, escrow) — простейший, классический пример смарт-контракта. С ее помощью не доверяющие друг другу контрагенты могут заморозить некоторую сумму монет в блокчейне таким образом, что в случае необходимости потратить эту сумму потребуются подписи более половины участников.

Смарт-контракты широко используются в сфере первичных распределений монет (ICO). Например, умный контракт может быть запрограммирован таким образом, что отправляя криптовалюту на кошелек проекта, участники краудсейла будут уверены, что в случае провала кампании их средства будут автоматически возвращены; если же финансовая цель ICO будет достигнута, то средства будут перечислены разработчикам. Однако сделано это будет при условии, что достаточное число участников мультиподписи (если она предусмотрена) активируют свои ключи, тем самым лично подтвердив добросовестность проекта.

К наиболее перспективным сферам применения смарт-контрактов многие эксперты относят финансовый рынок (банковские услуги, страхование, торговлю деривативами), бухгалтерский учет и аудит, управление цепями поставок и логистику, регистрацию прав собственности, всевозможные голосования, умный транспорт, цифровую идентификацию личности и т. д.

Подытожим

Написание смарт-контрактов - это достаточно новое направление, которое отличается от привычного программирования.

Технология Блокчейн имеет свои проблемы, разработчики пытаются устранить все возможные недостатки. Но она превосходит многие централизованные схемы, которые используются в банках и государственных структурах на данный момент. Очевидно, что умные контракты будут распространяться по всему миру в разных сферах жизнедеятельности, так как существенно экономят средства и время, а также дают возможность стереть границы со всеми странами мира в сфере коммерческой деятельности.

На текущем этапе развития смарт-контрактов стоит подробнее вникнуть в их суть, дабы не упустить невероятные возможности будущего.

Список литературы / References

1. Простокоин - Ваш проводник в мире криптовалют. [Электронный ресурс], 2018. Режим доступа: https://prostocoin.com/blog/ (дата обращения: 25.03.2018).
2. Журнал ForkLog - информационный ресурс о криптовалютах, блокчейне и децентрализованных технологиях. [Электронный ресурс], 2018. Режим доступа: https://forklog.com/ (дата обращения: 01.04.2018).