ВикипедиЯ

Смарт-контракт

Материал из Википедии — свободной энциклопедии

Смарт-контракт (англ. *Smart contract* — умный контракт) — компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн.

Содержание

Принцип работы

Стороны подписывают умный контракт, используя методы, аналогичные подписанию отправки средств в действующих криптовалютных сетях. После подписания сторонами контракт вступает в силу. Для обеспечения автоматизированного исполнения обязательств контракта непременно требуется среда существования, которая позволяет полностью автоматизировать выполнение пунктов контракта. Это означает, что умные контракты смогут существовать только внутри среды, имеющей беспрепятственный доступ исполняемого кода к объектам умного контракта. Все условия контракта должны иметь математическое описание и ясную логику исполнения. В связи с этим первые умные контракты имеют задачу формализации наиболее простых взаимоотношений, состоящих из небольшого количества условий. Имея беспрепятственный доступ к объектам контракта, умный контракт отслеживает по указанным условиям достижения или нарушения пунктов и принимает самостоятельные решения, основываясь на запрограммированных условиях. Таким образом, основной принцип умного контракта состоит в полной автоматизации и достоверности исполнения договорных отношений. [1]

История

Первые идеи умных контрактов были предложены в 1994 году Ником Сабо[2]. Практические реализации стали возможными, благодаря появлению в 2008 году технологии блокчейн[3]. Некоторые принципы умных контрактов были заложены в протоколе первой блокчейн-валюты Bitcoin[4], однако они не были реализованы в клиентском программном обеспечении, не обладали полнотой по Тьюрингу из соображений безопасности и не использовались на практике. С появлением технологии, стали высказываться идеи, что поверх протокола биткойна могут быть созданы различные протоколы более высокого уровня, включая полноценные умные контракты[5], по аналогии с тем как поверх TCP/IP существуют множество протоколов прикладного уровня.

Умные контракты впервые начали применяться на практике в проекте Ethereum. Идея создания проекта появилась в 2013 году. В тот момент основатель журнала Bitcoin Magazine Виталик Бутерин пришёл к выводу, что технология блокчейна может использоваться значительно шире, не только в криптовалютах. Он выдвинул идею универсальной децентрализованной блокчейн-платформы, в которой любой желающий может программно реализовать разные системы хранения и обработки информации. Главное условие — действия должны быть описаны как математические правила[6].

Объекты умного контракта

- **Подписанты** — стороны умного контракта, принимающие или отказывающиеся от условий с использованием электронных подписей. Прямым аналогом является подпись отправителя средств в сети Bitcoin, которая подтверждает внесение транзакции в цепочку блоков.
- **Предмет договора**. Предметом договора может являться только объект, находящийся внутри среды существования самого умного контракта, или же должен обеспечиваться беспрепятственный, прямой доступ умного контракта к предмету договора без участия человека. Это является наиболее сложным вопросом, который невозможно было решить до появления криптовалют в 2009 году.
- **Условия**. Условия умного контракта должны иметь полное математическое описание, которое возможно запрограммировать в среде существования умного контракта. Именно в условиях описывается логика исполнения пунктов предмета договора.
- **Децентрализованная платформа**. Для распределенного хранения смарт-контракта необходима его запись в Блокчейне этой платформы.[7]

Среда для работы умных контрактов

Для того, чтобы умные контракты могли существовать, требуются определённые условия:

1. Использование широко распространенных методов электронной подписи на основе публичных и приватных ключей (асимметричное шифрование).
2. Существование открытых, децентрализованных и доверительных сторонам контракта баз данных для исполняемых транзакций, работа которых полностью исключает человеческий фактор. Как пример: блокчейн в Bitcoin.
3. Децентрализация среды исполнения умного контракта. Как пример: Ethereum, Codius, Counterparty.
4. Достоверность источника цифровых данных. Как пример: корневые центры сертификации SSL в базах современных интернет-браузеров. [8]

Примеры

- По аналогии с IPO вводится первичное блокчейн-размещение (ICO англ. *initial coin offerings*) — метод краудфандинга для организации стартапов. На основе опубликованного меморандума инвесторы направляют средства на счет соответствующего умного контракта, получая взамен денежные знаки, играющие роль акций данного стартапа. По состоянию на август 2017 года объём инвестиций в ICO составляет $550 млн[9].
- Существует идея создания децентрализованного, основанного на Ethereum продукта, похожего на Facebook, где пользователи получат полный контроль над своими личными страницами, что даст им самим получать доходы от рекламы, вместо какой-либо компании.
- Возможность создания рынка ценных бумаг без участия фондовой биржи или клирингового центра. Для осуществления договоров не нужны ни услуги юристов, ни защищенные от несанкционированного доступа платформы для голосований, опросов, без необходимости вести подсчет голосов, без обработки бюллетеней избирательным органом и без участия социологического центра.

> *Первая большая и перспективная область развития блокчейна — финансовая. Это и криптовалюта, и смарт-контракты, и госреестры. Например, сейчас, чтобы продать дом, нужно несколько недель, а это может занимать всего 3 минуты.*

Виталик Бутерин, Москва, 30 августа 2017[10]

Перспективы

Сторонники умных контрактов утверждают[*кто?*], что многие их виды могут быть сделаны частично или полностью самовыполняемыми и самодостаточными. Умные контракты, основанные на криптографии, способны обеспечивать лучшую безопасность, чем традиционные контракты, основанные на праве, и снизить прочие трансакционные издержки, связанные с заключением договоров и возможных судебных издержек.

По мнению британского журнала The Economist умные контракты имеют перспективу стать наиболее важным приложением технологии блокчейн[9].

Юридическую значимость смарт-контракты могут получить при соответствии законам государства. Для этого нужно, чтобы смарт-контракты содержали условия и ограничения, установленные законодательством государства[11].

Недостатки

Наблюдатели выражают опасение, что распространение автоматизированных технологий поддержания контрактов может привести к ослаблению существующих социальных институтов, которые человечество создавало на протяжении многих поколений. Кроме того, такие технологии могут привести к исчезновению большого количества административных рабочих мест, также как роботизация привела к исчезновению рабочих мест в промышленности[9]. Это относится, в частности, к нотариусам, банковским служащим, а также к клеркам, занимающимся регистрацией сделок с недвижимым имуществом[12].

Небрежность разработчиков может повлечь за собой злонамеренное использование смарт-контрактов, как показала история с утечкой свыше трех миллионов монет Ethereum из проекта The DAO[13].

Примечания

1. Smart Contracts, Explained (https://cointelegraph.com/explained/smart-contracts-explained)
2. Smart Contracts (http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html). *www.fon.hum.uva.nl*.
3. http://bitcoin.org/bitcoin.pdf
4. Как на самом деле работает протокол Биткоин / Geektimes (https://geektimes.ru/post/222493/)
5. RSK (http://rootstock.io)
6. Создатель Ethereum Виталик Бутерин: «Блокчейн поможет искоренить коррупцию» (https://incrussia.ru/blockchain/sozdatel-ethereum-vitalik-buterin-blokcheyn-pomozhet-iskorenit-korruptsiyu/)
7. Смарт-контракты, пояснения (https://cointelegraph.com/explained/smart-contracts-explained)
8. Смарт-контракты: как использовать и насколько надежны для сделок (https://cryptonet.biz/ru/smart-kontrakty-kak-ispolzovat-i-naskolko-nadezhny-dlya-sdelok/)
9. «If blockchains ran the world» (http://worldif.economist.com/article/13525/disrupting-trust-business), The Economist, 6 July, 2017
10. Виталик Бутерин: «Путин знает, что такое блокчейн — это и есть хайп» (https://rb.ru/opinion/buterin-rock-and-roll/)
11. Из блокчейна слов не выкинешь: как он изменит Украину и почему опыт других стран нам уже не подходит (http://businessviews.com.ua/ru/tech/id/iz-blokchejna-slov-ne-vykinesh-kak-on-izmenit-ukrainu-i-pochemu-opyt-drugih-stran-nam-uzhe-ne-podhodit-1689/) (укр.). businessviews.com.ua. Проверено 9 апреля 2018.
12. Профессионал года — создатель криптовалюты Ethereum Виталик Бутерин (https://www.vedomosti.ru/technology/articles/2017/12/28/746767-professional-goda-vitalik-buterin) «Ведомости», 28.12.2017
13. Уроки DAO: куда приводят мечты | ForkLog (https://forklog.com/uroki-dao-kuda-privodyat-mechty/) (рус.). forklog.com. Проверено 9 апреля 2018.

Ссылки

- Умные контракты (Четвертая революция стоимости) (http://old.computerra.ru/1998/266/194332/) — статья Ника Сабо, Компьютерра 1998 год.
- The Idea of Smart Contracts (https://web.archive.org/web/20060615044959/http://szabo.best.vwh.net/smart_contracts_idea.html)

- erights.org: Smart Contracts (http://www.erights.org/smart-contracts/)
- «Late on payments? (https://web.archive.org/web/20071009185738/http://www.venturacountystar.com/vcs/bravo/article/0,1375,VCS_1798_4769614,00.html) Device won't let car engine start.» (https://web.archive.org/web/20071009185738/http://www.venturacountystar.com/vcs/bravo/article/0,1375,VCS_1798_4769614,00.html)
- Open-Transactions: open-source Smart Contracts (http://opentransactions.org/wiki/index.php?title=Smart_contracts)
- Все, что нужно знать об умных контрактах (https://rb.ru/story/smart-contract/) / rb.ru, 2017
