СЕМАНТИЧЕСКИЕ «УМНЫЕ» КОНТРАКТЫ

Дмитрий СВИРИДЕНКО, д.ф.-м.н., профессор

(ИМ СО РАН, НГУ, Группа компаний АЙЛАЙН)

Напомним, что сама идея умных контрактов, как идея роботизации «деловых» отношений *агентов/акторов* (в роли которых могут выступать люди, оборудование, программы, бизнес-процессы и т.п.), была высказана еще в 90-е годы прошлого столетия, но получила свое практическое воплощение сравнительно недавно и сразу же привлекла к себе пристальное внимание, поскольку было понятно, что эта инновация обладает огромным потенциалом и способна совершить настоящую революцию в сфере автоматизации управления широкого спектра деловых отношений. Однако, как справедливо отмечают многие специалисты, быстро выяснилось, что в том виде, в котором «на свет» появились «умные» контракты, а также те инструменты, которыми они создаются и исполняются, позволяет говорить только об относительно полной автоматизации и роботизации очень узкого и весьма специализированного спектра деловых отношений.

Одной из причин этого является то, что понятие «умного» контракта нашло свое *первое* практическое воплощение в сети Биткоин, ставшее для последующих «криптовалютных» проектов неким эталоном. Напомним, что в системе Биткоин «умный» контракт трактуется как любой *транзакционный протокол*, чей базовый функционал не должен зависеть от *доверия* к третьим лицам, что обеспечивалось используемой в сети технологией блокчейн. Такое достаточно жесткое и весьма ограниченное понимание «умного» контракта привело к тому, что в современном «криптовалютном» мире от смарт-контракта требуется, чтобы никто не имел возможность вмешиваться и изменять его исполнение и, тем самым, влиять на жестко запрограммированное поведение всей децентрализованной системы. Другими словами, речь идет о тотальном изгнании понятия «доверия» из формализуемых смарт-контрактами деловых отношениях, что, мягко говоря, представляется не вполне разумным. Более того, во многих публикациях, посвященных теме смарт-контрактов, данное обстоятельство подается как исключительное достоинство и преимущество, а в отдельных статьях контракты, допускающие присутствие в своих условиях тех или иных элементов доверия, предлагается вообще именовать *тупыми*.

Автор считает, что подобное трактовка понятия «умного» контракта является неправильной и обязательно приведет (да и уже фактически привела) к значительному сужению спектра практического его применения. Выход здесь видится в методологической и инструментальной возможности учитывать и находить баланс интересов всех участников контракта при его формализации и исполнении. Такая возможность может быть реализована, например, путем широкого использования в языке написания контрактов *оракулов* – специальных каналов взаимодействия контракта с внешним миром.

Другой причиной современной чрезвычайно узкой интерпретации и ограниченного применения понятия «умного» контракта послужило то обстоятельство, что в качестве инструментальных средств написания смарт-контрактов предлагается использовать языки *императивного программирования*, «генетически» и жестко сопряженные с технологиями распределенного реестра и стратегиями достижения консенсуса, что повлекло за собой разрушение того исходного смысла (*семантики*), который предполагалось придавать контрактам как формальным конструкциям, описывающим деловые отношения между агентами/акторами. Смысл и логическая структура контракта, соответствующие его декларативному аспекту «что», как-бы растворились в программном коде, превратившись в императивное "как", в силу чего программный код контракта стал практически недоступным для понимания специалистам, не знакомых с программированием. В связи с этим возникает вопрос – как такие контракты следует использовать в повседневном бизнесе? Ведь на практике очень важно, чтобы смарт-контракты интуитивно воспринимались бизнес-участниками как обычные контракты, но только более строго и четко оформленные. Кстати, заметим, что программный императивный код контракта не может быть полезным и для его автоматической верификации. Причина в том, что если используется полный по Тьюрингу язык программирования (например, язык Solidity), то получаемый код контракта не доступен для автоматической его верификации в силу алгоритмической неразрешимости этой проблемы в таком языке.

Выше мы упоминали о наличии жесткой привязки существующих смарт-контрактов и соответствующих им императивных инструментальных средств программирования к встроенной в систему технологии распределенных реестров. Такая привязка может оказаться, как это не покажется странным, большим психологическим барьером для широкого распространении концепции смарт-контракта. Причин тому несколько. Во-первых, некоторым участникам контрактного соглашения может показаться опасным вывод конфиденциальной информации, содержащейся в контракте, во внешний мир, и потому данное обстоятельство обязательно нужно учитывать при проектировании логических условий контракта и схемы его функционирования. Во-вторых, жесткая привязка к единственному виду блокчейна может оказаться весьма обременительным условием, поскольку в разных ситуациях оптимальное решение может быть связанным с совершенно другой формой распределенного реестра. Поэтому более правильным видится предоставление пользователю возможности не только самому проектировать смарт-контракт, в том числе и путем выбора наиболее подходящего готового *шаблона*, но и определять режим использования контрактом конфиденциальной информации, а также выбирать конкретный вид реестра для каждого своего решения, что потребует от инструментальных средств написания смарт-контрактов развитых языковых средств и определенной независимости от используемых видов реестров.

Естественно возникает вопрос – как преодолеть указанные выше недостатки и обойти проблемы, присущие текущему пониманию и практическому воплощению понятия «умного» контракта? По мнению автора, ответ следует искать, прежде всего, в отказе от использования для написания умных контрактов Тьюрингово

полных *императивных языков программирования* и использования для этих целей специальных *декларативных языков спецификаций*, не обязательно Тьюрингово полных, но позволяющих контракт представлять в виде некой вычислимой и, тем самым, *исполнимой* компьютером *модели*, достаточно полно и адекватно описывающую *предметную область*, к которой относится контракт, и сложную *логику* его исполнения. Другими словами, предлагается смарт-контракты не программировать, а ***моделировать***! При этом естественно требовать, чтобы такая модель обязательно содержала в себе и наглядно представляла исходную *семантику*.

Подобный *семантический смарт-контракт* представляет собой автоматически управляемое и юридически правомерное соглашение, сохраняющее смысл (семантику) деловых взаимоотношений агентов/акторов и предназначенное для компьютерного исполнения (возможно с применением криптографических и иных средств). Если обычные контракты определяют условия взаимодействия партнеров с помощью юридически значимых текстовых документов, то семантический смарт-контракт, как формальная логико-вероятностная модель, будет это делать с помощью либо полностью автоматического, либо с использованием оракулов частично автоматического сопровождения и поддержки контрактных операций, при необходимости сохраняя историю их исполнения в том или ином, наиболее подходящем для текущей ситуации распределенном реестре.

В качестве такого конкретного языка спецификаций контрактных отношений автор предлагает использовать *логико-вероятностный язык Δ_0-формул*, развиваемый специалистами Института математики СО РАН и Иркутского государственного университета в рамках *концепции семантического моделирования*. На базе этого языка в настоящее время создано несколько его диалектов. Примером здесь может служить язык Libretto, созданный и успешно применяемый на практике иркутской группой ученых и специалистов во главе с профессором Манцивода А.В., и комплекс Discovery д.ф.-м.н. Витяева Е.Е., позволяющий моделировать логико-вероятностные контрактные условия.

При создании и последующем использовании языков семантического моделирования полностью подтвердилось, что переход от *программирования* «умного» контракта к его *моделированию* в виде *семантической логико-вероятностной* Δ_0*-модели* позволяет гарантированно преодолевать указанные ранее препятствия и устранять недостатки, открывая тем самым новые горизонты развития и возможности дальнейшего совершенствования понятия смарт-контракта. Например, появляется возможность организовывать и развивать на принципиально иной методологической, теоретической и технологической основе различные *децентрализованные сообщества* (экосистемы) и проводить ICO. Следует отметить, что именно такой вариант расширенного понимания понятия умного контракта и соответствующий ему диалект языка семантического моделирования реализуется в настоящее время в рамках проекта MiniApps.pro.

Другой важной областью применения концепции семантических смарт-контрактов является тема «умных» кошельков. Этой прикладной и весьма актуальной теме будет посвящена отдельная статья автора.