БАНКОВСКАЯ СИСТЕМА И БАНКОВСКАЯ ДЕЯТЕЛЬНОСТЬ

В. М. Камалян*

Правовые риски использования цифровых технологий в банковской деятельности[1]

Аннотация. *В работе автор на основе анализа правовых рисков использования смарт-контрактов в банковской деятельности делает вывод о необходимости специального правового регулирования использования цифровых технологий в банковской деятельности, которое позволило бы минимизировать рассмотренные правовые риски. Автор полагает, что подобное правовое регулирование в целях минимизации правовых рисков должно определять смарт-контракт не как конструкцию договора, заключенного в письменной форме, а как способ исполнения обязательств. Анализируя правовые риски, связанные с идентификацией личности при внедрении цифровых технологий в банковскую деятельность, автор предлагает использование блокчейн-технологии как основу системы идентификации клиентов, при этом используя исключительно преимущественные возможности данной технологии с соблюдением требований международных стандартов и национального законодательства о противодействии отмыванию доходов, полученных преступным путем, и финансированию терроризма. Данное решение позволит упростить и защитить систему идентификации и обработки данных о клиентах банков, однако оно требует эффективной государственной поддержки и правового регулирования.*

Ключевые слова: *цифровые технологии, финансовые технологии, цифровизация, цифровой банкинг, правовые риски, смарт-контракт, правовая природа смарт-контракта, блокчейн, идентификация, отмывание преступных доходов, финансирование терроризма.*

DOI: 10.17803/1994-1471.2019.103.6.032-039

Банковская деятельность является самым динамично развивающимся сегментом экономики. Одним из способов развития банковского рынка является широкое внедрение в деятельность кредитных организаций новых банковских технологий. В условиях активной цифровизации, связанной с появлением новых финансовых технологий, открываются новые перспективы использования цифровых технологий в банковской деятельности, позво-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16203 мк на тему «Российское и зарубежное право об использовании цифровых технологий в банковской деятельности и практика его применения: сравнительно-правовой аспект».

* *Камалян Владислав Михайлович*, аспирант Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
vladkamalyan@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

ляющие решать ряд важных как для кредитной организации, так и для ее клиентов задач:

— снижение операционных расходов банка и его клиента;
— повышение скорости совершения операций;
— снижение трудоемкости процессов совершения банковских операций;
— минимизация банковских рисков;
— повышение прозрачности совершения операций и рост уровня доверия к кредитным организациям;
— повышение качества обслуживания клиентов.

Подобного рода задачи постоянно возникают перед кредитными организациями. Когда появляется технология, которая позволяет в определенной мере решить данные задачи, любой банк должен быть заинтересован в ее внедрении в банковскую деятельность. Однако кредитная организация также должна осознавать, с какими правовыми рисками она может столкнуться при внедрении цифровых технологий. Поэтому необходимо постоянно анализировать подобные риски и искать пути их минимизации. Одними из самых существенных правовых рисков внедрения цифровых технологий в банковскую деятельность являются риски, связанные с использованием смарт-контракта, а также риски проблемной идентификации клиента.

1. ПРАВОВЫЕ РИСКИ ИСПОЛЬЗОВАНИЯ СМАРТ-КОНТРАКТА В БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Технология смарт-контракта является совершенно новой для всего мира, и ее появление тесно связано с активным развитием блокчейн-технологий. Разумеется, на такое развитие не могут не реагировать как представители государственной власти разных государств, так и представители научных и банковских сообществ. В российском банковском праве пока отсутствует упоминание о смарт-контрактах, а теоретическая концепция внедрения данного понятия в правовую систему еще основательно не разработана. Вместе с тем цифровизация банковской деятельности определенно требует разработки доктринальной концепции смарт-контрактов, в рамках которой необходимо выявить правовые риски использования смарт-контрактов в банковской деятельности. Смарт-контракт можно определить как программный код, полностью или частично отражающий и автоматически исполняющий заключенный между участниками договор на базе технологии распределенного реестра данных.

Рассмотрим правовые риски использования смарт-контракта на следующем примере. Британский банк Barclays использовал смарт-контракты для проведения сделок с аккредитивами в рамках международной поставки товаров (сыра и сливочного масла). В состав документов, подтверждающих исполнение условий аккредитива, вошли электронные документы: сертификат происхождения товара, страховой сертификат, счет, товарно-транспортная накладная[2]. Сто́ит отметить, что подробности данной сделки и особенности ее оформления публично неизвестны, поскольку составляют коммерческую тайну сторон. Поэтому нижеследующие суждения не следует применять к фактической стороне данной сделки.

Если смарт-контракт считать договором, то в данном случае смарт-контракт может представлять собой как минимум основной договор между поставщиком и покупателем, но также может являться и смешанным договором, включающим в себя следующие элементы: основной договор между поставщиком и покупателем, договор между покупателем и банком-эмитентом о выдаче аккредитива, договор между банком-эмитентом и исполняющим банком, содержащий полномочие совершить платеж. Кроме того, допустимо заключать несколько смарт-контрактов на исполнение отдельных указанных выше обязательств по основному договору и аккредитиву.

В рамках данной операции возможны следующие правовые риски.

[2] Аналитический обзор Центрального Банка РФ по теме «Смарт-контракты» от октября 2018 г. С. 10 // Сайт Центрального Банка РФ. URL: http://www.cbr.ru/content/document/file/47862/smartkontrakt_18-10.pdf (дата обращения: 23.03.2019).

Во-первых, смарт-контракт — технологически сложное явление, представляющее собой программный код, написанный на языке компьютера. Поэтому для составления смарт-контракта всегда привлекается специалист, имеющий достаточную техническую квалификацию. Такой специалист едва ли владеет юридической техникой, чтобы всегда верно отражать действительную юридическую волю сторон в программном коде. Поэтому с первым правовым риском использования смарт-контракта стороны сталкиваются уже на стадии его составления: специалист, не обладающий юридическим образованием, не всегда способен в точности отразить юридическую волю сторон по сделке. В итоге исполнение смарт-контракта может привести к иным результатам, вопреки воле сторон. Например, специалист может не придать должного значения товарно-транспортным накладным и не включить условия о получении программой данных об этом документе в смарт-контракт. Как следствие, покупатель не получает данные о товарно-транспортной накладной, которая является важным документом бухгалтерской отчетности. Впоследствии покупателю необходимо дополнительно запрашивать у поставщика документы, что занимает определенное время и требует определенных расходов.

Второй существенный правовой риск использования смарт-контракта заключается в возможности технической ошибки, допущенной специалистом при составлении смарт-контракта. Любая техническая ошибка в коде, будь это даже пропущенный символ или цифра, способна привести к неправильному ходу исполнения смарт-контракта или даже к полной остановке, сбою. Запущенный смарт-контракт невозможно изменить, исправить или дополнить ввиду особенностей его технической природы, построенной на технологии блокчейн[3]. Поэтому код, заложенный в смарт-контракт, должен быть технически идеален, чтобы программа смогла произвести алгоритм действий от начала до самого конца.

В случае ошибки хода смарт-контракта стороны могут столкнуться со следующими правовыми проблемами. В первую очередь это неисполнение обязательства стороны. В указанном выше примере допускаем, что ввиду ошибки в смарт-контракте деньги не поступили на счет бенефициара (поставщика), то есть покупатель, хотя и не преднамеренно, не исполнил обязательство по оплате товара. Поставщик в таком случае будет предъявлять требования именно к покупателю[4], несмотря на вину специалиста, допустившего техническую ошибку при составлении смарт-контракта. Покупатель оказывается в такой ситуации, что должен оплатить полученный товар другим путем. Более того, если денежные средства были также заложены в смарт-контракт и заблокированы им, покупателю придется искать новые финансовые возможности, чтобы погасить образовавшуюся задолженность, при этом претерпев убытки в размере заблокированных денежных средств. Поэтому в данном случае стороны могут нести не только правовые, но и финансовые риски.

Третий немаловажный правовой риск связан с ситуацией возникновения споров между сторонами. Смарт-контракт способен минимизировать вероятность возникновения споров ввиду автоматизации исполнения обязательства, но свести к нулю такую вероятность теоретически невозможно. Тем не менее, продолжая ситуацию с неисполнением покупателем обязательств по оплате товара, дополним ее следующими условиями: поставщик обратился в суд с требованием взыскать денежные средства. Суд запросит договор, на основании которого возник спор. И в данном случае ситуация имеет два направления развития в зависимости от того, считать ли смарт-контракт непосредственно договором[5]. Если его считать таковым, то поставщику необходимо будет предоставить

[3] *Ефимова Л. Г.*, *Сиземова О. Б.* Правовая природа смарт-контракта // Банковское право. 2019. № 1. С. 24.

[4] *Савельев А. И.* Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. С. 102.

[5] *Городов О. А.*, *Егорова М. А.* Основные направления совершенствования правового регулирования в сфере цифровой экономики в России // Право и цифровая экономика. 2018. № 1 (01). С. 9.

смарт-контракт суду. Однако единственное, что он сможет предоставить, — это код смарт-контракта. Судья — человек с юридическим образованием, не сведущий в программировании, — не сможет принять текст кода как надлежащее доказательство основания спорных взаимоотношений[6]. Поставщик в таком случае оказывается в ситуации, что он фактически ничего не может предоставить суду в подтверждение заявленных доводов. Суд потребует надлежащую письменную форму договора, в противном случае истца ждет отказ в удовлетворении исковых требований. Таким образом, поставщик оказывается лишенным правовой защиты. Ситуация складывается иначе, если смарт-контракт считать не договором, а лишь средством его исполнения. В таком случае наряду со смарт-контрактом составляется обычный письменный договор, который закрепляет волю сторон на человеческом языке, понятном как для самих сторон, так и для судьи. Следовательно, интересы потерпевшей стороны всегда будут защищены в суде. Таким образом, данный правовой риск возможно и необходимо избегать путем заключения обычного письменного договора.

Сто́ит отметить, что данный способ позволит минимизировать и ранее указанные риски. В частности, обычный письменный договор можно предоставить специалисту для удобства составления смарт-контракта, и тогда текст будет в максимальной степени коррелировать с программным кодом. Таким образом, риск неправильного отражения воли сторон в смарт-контракте минимизируется за счет письменного отражения воли сторон на бумажном носителе.

Более того, обычный письменный договор позволит минимизировать правовые и финансовые риски, возникающие при неправильном ходе исполнения смарт-контракта: представляется, что помимо основного договора поставки необходимо заключать договор со специалистом, который будет составлять смарт-контракт и, самое главное, нести ответственность за неправильное его составление. В случае, когда из-за технической ошибки смарт-контракт не исполнил обязательство покупателя по оплате товара, вина лежит на специалисте и ответственность нести должен тоже он. В случае если специалист является штатным сотрудником одной из сторон, конечно, ответственность будет нести та сторона, в штате которой данный специалист работает.

Более того, как уже отмечалось, условия смарт-контракта невозможно поменять или отменить. Можно предполагать, что нормы гражданского права об изменении и о расторжении договора неприменимы к смарт-контракту. Поэтому представляется, что это было бы грубым нарушением принципов гражданского права, в связи с чем нельзя приравнивать смарт-контракт к договору. Отсюда вытекает еще один правовой риск использования смарт-контракта, связанный с возможностью изменения или отмены смарт-контракта, если, предположим, смарт-контрактом была исполнена противоправная сделка. Например, покупатель приобрел квартиру в ипотеку у собственника без согласия супруги последнего. Смарт-контракт выполнил следующие действия: перечислил кредитные денежные средства банка на счет заемщика-покупателя и затем, получив данные об успешной регистрации нового права собственности на квартиру, перевел денежные средства плательщика на счет продавца. Возникает необходимость в реституции прав сторон, но как это сделать, если процесс смарт-контракта необратим и его невозможно изменить? Представляется, что существует два варианта реституции прав в данной ситуации: традиционный или посредством смарт-контракта. При традиционном варианте реституция денежных обязательств происходит посредством традиционных форм расчетов: продавец возвращает деньги покупателю, покупатель возвращает ипотечный кредит банку. Регистрационная запись о праве собственности на квартиру на основании решения суда отменяется Росреестром, что восстанавливает права прежнего собственника на квартиру. Обратные действия можно также совершить в добровольном порядке посредством уже нового смарт-контракта, аналогичного пре-

[6] *Савельев А. И.* Указ. соч. С. 94—117.

дыдущему, но уже с другими сторонами — плательщиком и получателем.

Таким образом, с правовой точки зрения крайне опасно считать смарт-контракт договором: чтобы все стороны имели правовую защиту своих интересов, необходимо традиционное письменное заключение договора, причем не только основного, но и с составителем смарт-контракта. Поэтому признание смарт-контракта договором является фактором, приводящим к росту правовых рисков использования данной технологии в банковской деятельности. В связи с этим необходимо законодательно установить, что смарт-контракт не является договором, заключенным в письменном виде, не отражает волю сторон и является лишь инструментом исполнения обязательств. Тогда и практика применения смарт-контракта, и правоприменительная практика не будут двойственными, что позволит более эффективно внедрять данную технологию в банковскую деятельность.

2. ПРАВОВЫЕ РИСКИ ИДЕНТИФИКАЦИИ В ЦИФРОВОМ БАНКИНГЕ

Современная банковская деятельность базируется на основополагающем принципе KYC (Know Your Client — Знай своего клиента), значение которого состоит в идентификации банком клиентов, а также бенефициаров банковских операций. Данный принцип сформулирован как в Международных стандартах по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения, принятых ФАТФ[7], так и во многих национальных правовых системах, в частности в России — в Федеральном законе от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[8], а также в Положении об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (утв. Банком России 15.10.2015 № 499-П)[9]. Основная задача данного принципа — это борьба с легализацией преступных доходов и финансированием терроризма. При внедрении цифровых технологий в банковскую деятельность важно не допустить нарушения данных принципов. Опасения в данном случае совсем не безосновательны по следующим причинам.

Если говорить о внедрении такой технологии, как блокчейн, то сто́ит отметить, что блокчейн основан на полной анонимности: стороны транзакций не знают друг о друге ничего, кроме того, что они передают друг другу. К сожалению, сегодня блокчейн уже активно применяется и в противоправных целях. Существует так называемый даркнет (DarkNet), базирующийся на технологии блокчейн, где участники могут совершенно легко и, главное, анонимно приобрести оружие, наркотики, поддельные документы и много другое. Все транзакции происходят через криптовалюту, отследить участников сделки практически невозможно благодаря асимметричному шифрованию. Данный пример показывает, как блокчейн уже способствует развитию легализации преступных доходов и финансированию терроризма. Поэтому возникает вопрос, как банку внедрить блокчейн в свое программное обеспечение, чтобы не нарушать законодательство о противодействии легализации преступных доходов и финансированию терроризма. Именно данный риск является существенным правовым

[7] П. 10 Раздела D Рекомендаций ФАТФ Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения — Перевод подготовлен Международным учебно-методическим центром по финансовому мониторингу, Вече, 2012 — Опубликовано на сайте Росфинмониторинга http://www.fedsfm.ru/content/files/documents/fatf/рекомендации%20фатф.pdf, дата обращения:23.03.2019 г.

[8] Российская газета. № 151—152. 09.08.2001.

[9] Вестник Банка России. № 115. 16.12.2015.

риском внедрения технологии блокчейн в банковскую деятельность.

Таким образом, банкам необходимо найти определенный компромисс между преимуществами блокчейна и требованиями законодательства, чтобы эффективно применять данную технологию.

В частности, таким компромиссом является включение блокчейн-технологии в процесс идентификации, точнее — перевод процесса идентификации на блокчейн-технологию. Необходимо разработать и законодательно утвердить систему идентификации личности, основанную на блокчейне, где все данные личности будут оцифрованы и зашифрованы, вследствие чего защищены. Посредством блокчейна данные могут передаваться в том числе банку, причем моментально и комплексно. Сто́ит отметить, что такая система позволит защитить персональные данные клиента, не допустив незаконной утечки или передачи данных, поскольку система децентрализована и асимметрично зашифрована. Сегодня на частном уровне уже разрабатываются подобные системы.

Так, например, модель Civic позволяет (в случае возникновения такой необходимости) обеспечить безопасный и более дешевый доступ к проверке подлинности личности с помощью блокчейн-технологии. Проверку личной информации больше не нужно будет проходить заново каждый раз, когда требуется регистрация в новом приложении или сайте. И все это без фактического сбора и хранения пользовательской информации со стороны компании. Блокчейн здесь используется для защиты данных. Эти данные по всей строгости проверены Civic или другими партнерскими системами идентификации, а затем засвидетельствованы и привязаны к блокчейну в виде данных, не поддающихся дешифровке. Эти данные обмениваются исключительно между пользователем и определенным контрагентом с помощью Civic tokens (CVC). Участниками сети могут быть банки, финансовые сервисы, организации сферы здравоохранения и другие надежные организации. Civic уже имеет рабочий продукт проверки подлинности, который доступен во всем мире и получил премию «Лучший новый стартап» на конференции «Идентификация пользователей» в 2017 г.[10]

uPort — еще одно решение для управления идентификацией, разработанное престижной компанией Blockchain ConsenSys. Главная цель разработчиков uPort — создание элементарной в использовании системы идентификации личности на базе блокчейна Эфириум. Система uPort рассматривает мобильный телефон человека как продолжение его собственного «я». Во время первичной настройки системы с вашего разрешения она извлекает данные из телефона и записывает смарт-контракт на их основе. В дальнейшем им можно пользоваться по мере необходимости.

Данная платформа в конце 2017 г. стала доступна не отдельно взятому лицу, а целому городу. Речь идет о швейцарском Цуге, именуемом «Криптодолиной». Вот уже несколько месяцев реализуется программа регистрации удостоверений для жителей города на основе блокчейна. Это позволит людям получить доступ к электронным услугам, таким как подтверждение проживания и онлайн-голосование. Система должна ознаменовать собой новую ветвь развития блокчейна, поскольку она демонстрирует, что с помощью данной технологии городское правительство может осуществлять цифровую проверку граждан[11].

Таким образом, технология блокчейн представляет собой как риск возникновения проблемы идентификации клиентом банка, так и решение данной проблемы. Сто́ит отметить, что сегодня идентификация клиента основана на государственных и международных стандартах. Поэтому до тех пор, пока блокчейн-технологии не будут законодательно одобрены для целей идентификации как на государственном, так и на международном уровне, банки не рискнут менять систему идентификации самостоятельно.

[10] Системы идентификации личности на базе блокчейна. 24.02.2018 // URL: https://cryptogu.ru/sistemy-identifikacii-lichnosti-na-baze-blokchejna/ (дата обращения: 23.03.2019).

[11] Системы идентификации личности на базе блокчейна.

Таким образом, можно сделать следующие выводы:

1. Внедрение цифровых технологий в банковскую деятельность требует специального правового регулирования с целью минимизации правовых рисков их использования.

2. В целях минимизации правовых рисков смарт-контракт не сто́ит приравнивать к договору: данная технология является лишь средством исполнения обязательств.

3. Правовые риски использования смарт-контракта во многом связаны с лицом, осуществляющим разработку смарт-контракта, в связи с чем необходимо установить правовой статус и ответственность такого лица.

4. Правовые риски идентификации личности в банковской деятельности могут быть минимизированы за счет внедрения цифровых технологий в правильном русле.

5. Внедрение цифровых технологий в банковскую деятельность требует особой государственной поддержки в рамках эффективного правового регулирования, позволяющего сочетать пользу цифровых технологий и публичные интересы государства.

БИБЛИОГРАФИЯ

1. *Городов О. А.*, *Егорова М. А.* Основные направления совершенствования правового регулирования в сфере цифровой экономики в России // Право и цифровая экономика. — 2018. — № 1 (01). — С. 6—11.
2. *Ефимова Л. Г.*, *Сиземова О. Б.* Правовая природа смарт-контракта // Банковское право. — 2019. — № 1. — С. 21—27.
3. *Савельев А. И.* Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. — 2017. — № 5. — С. 94—117.

Материал поступил в редакцию 6 мая 2019 г.

LEGAL RISKS OF USING DIGITAL TECHNOLOGIES IN BANKING[12]

KAMALYAN Vladislav Mikhailovich, Postgraduate Student of the Kutafin Moscow State Law University (MSAL)
vladkamalyan@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *Based on the analysis of legal risks of using smart contracts in banking activities, the author concludes that there is a need for special legal regulation of the use of digital technologies in banking, which would minimize the legal risks examined in the paper. The author believes that such legal regulation in order to minimize legal risks should define a smart contract as a way of fulfillment of obligations rather than as a design of a contract concluded in writing. Analyzing the legal risks associated with the person identity during the introduction of digital technologies in banking, the author suggests the use of blockchain technology as the basis of the system of identification of customers using exclusively the advantages of this technology in compliance with the requirements of international standards and national legislation regulating counteraction to laundering of proceeds of crime and financing of terrorism. This solution will simplify and protect the system of identification and processing of data regarding the clients of banks, but it requires effective state support and legal regulation.*

[12] The research was carried out with the financial support of RFBR within the framework of the scientific project No. 18-29-16203 mk on the topic «Russian and Foreign Law on the Use of Digital Technologies in Banking and the Practice of its Application: Comparative Law Aspect».

Keywords: *digital technologies, financial technologies (fintech), digitalization, digital banking, legal risks, smart contract, legal nature of a smart contract, blockchain, identification, laundering of proceeds of crime, financing of terrorism.*

REFERENCES (TRANSLITERATION)

1. *Gorodov O. A.*, *Egorova M. A.* Osnovnye napravleniya sovershenstvovaniya pravovogo regulirovaniya v sfere cifrovoj ekonomiki v Rossii // Pravo i cifrovaya ekonomika. — 2018. — № 1 (01). — S. 6—11.
2. *Efimova L. G.*, *Sizemova O. B.* Pravovaya priroda smart-kontrakta // Bankovskoe pravo. — 2019. — № 1. — S. 21—27.
3. *Savel'ev A. I.* Nekotorye pravovye aspekty ispol'zovaniya smart-kontraktov i blokchejn-tekhnologij po rossijskomu pravu // Zakon. — 2017. — № 5. — S. 94—117