

## Проблемы и перспективы реализации технологии блокчейн в банковской сфере

**Биченов Михаил Юрьевич** – магистр Финансового университета при Правительстве РФ.

*Аннотация:* В данной статье автором проведен анализ технологии блокчейн. Рассмотрены основные проблемы и перспективы внедрения данной системы в банковскую сферу. Автором были рассмотрены основные преимущества системы блокчейн. Проанализированы банковские проекты. На основании данного исследования сделан вывод о том, что Федеральной службе безопасности в рамках своих полномочий целесообразно предусмотреть критерии и требования, предъявляемые к системам блокчейн.

*Ключевые слова:* Блокчейн, банковские системы, технологии.

В последние годы активно обсуждается технология, получившая название блокчейн. Во многом, известность данной технологии принес успех, так называемых, криптовалют. Тем не менее, непосредственно система блокчейн также имеет самостоятельную ценность, так как обладает рядом несомненных преимуществ, фактически, не имеющих аналогов на сегодняшний день. Достаточно скоро такие преимущества были отмечены участниками финансового рынка, в особенности, кредитными организациями.

Заинтересованность участников финансового рынка в технологии блокчейн и значительный прогресс в сфере цифровой экономики определяют необходимость разработки правовых инструментов, позволяющих интегрировать систему блокчейн в экономику государства.

Для исследования вопроса возможности и перспектив внедрения системы блокчейн в банковском секторе необходимо определить сущность системы блокчейн.

Не прибегая к специальным техническим знаниям, систему блокчейн можно

охарактеризовать как базу данных безопасных транзакций (записей), которая является общей и автономной для всех участников функционирующей сети. При этом в сети участники системы действуют независимо, и каждый из них полагается только на собственную информацию в системе.

Из представленного определения следует несколько основных характеристик системы блокчейн. Во-первых, система блокчейн состоит из безопасных транзакций. Безопасность таких транзакций объясняется главной особенностью системы блокчейн – каждая последующая транзакция (запись) в общей базе данных ссылается на предыдущую и так по цепочке досамой первой. Сама же транзакция (запись) выражается в виде специального хэш-кода – индивидуального набора символов, позволяющим идентифицировать то или иное действие. Такая идентификация возможна посредством системы ключей – публичного и приватного ключа. Публичный ключ позволяет идентифицировать лицо, относящееся к системе, достоверно определить, что действие осуществляет конкретно определенное лицо. Приватный ключ фактически дает полный доступ к системе участнику, в том числе, предоставляет возможность дешифровать соответствующий хэш-код.

Таким образом, безопасность, фактически, обеспечивается совокупностью двух факторов: безопасность первичной записи посредством использования системы индивидуального шифрования и безопасность системы целиком, ввиду невозможности изменения транзакции (записи) без изменения всех записей в системе.

Вторая характеристика системы блокчейн это ее одновременная общность (вся информация идентична для всех участников системы) и автономность (каждый участник системы обладает собственной версией цепочки записей, которая признается оригинальной, то есть, каждый участник опирается только на собственную информацию без необходимости получения подтверждения действительности такой информации). Такая характеристика обеспечивается спецификой процесса функционирования системы.

При совершении транзакций один из участников системы отправляет зашифрованное сообщение (фактически, это любая запись, в том числе, транзакция в виде хэш-кода) с публичным ключом в, так называемый, пул неподтвержденных транзакций. Далее, специальные участники системы, «майнеры», с помощью технических средств осуществляют формирование транзакций (записей) в блоки, которые, в свою очередь, формируются в более крупные блоки и так далее, пока не будет сформирован блок установленного объема, который, фактически, является одним из звеньев общей цепи

(вся условная цепь данных и является непосредственно самой системой блокчейн). Полученные звенья доводятся до всех участников системы, в результате чего, каждый из них обладает полным набором сведений о сложившихся транзакциях в рамках данного, равно как и всех предыдущих звена.

Третьей характеристикой системы блокчейн является то, что данная система доступна только ее участникам. Данная характеристика наряду с вышеуказанными характеристиками также является крайне ценной особенностью, так как позволяет формировать гибкий подход к построению системы, ее целей и индивидуальных особенностей, в том числе, с учетом потребностей участников системы, которыми могут являться, например, клиенты банковского сектора.

Осознавая преимущества технологии блокчейн еще в 2016 году наиболее крупными субъектами банковского сектора, включая Банк России, была представлена блокчейн платформа «Мастерчейн», в рамках которой по сегодняшний день ведутся разработки проектов, основанных на технологии блокчейн. Однако, как отмечается разработчиками и участниками проекта «Мастерчейн», на сегодняшний день невозможно в полной мере реализовать потенциал системы блокчейн, главным образом, по причине отсутствия надлежащего правового регулирования, в результате чего разрабатываемых проектов всего несколько и, кроме того, указанные проекты несколько ограничены функционально. В то же время, такие промежуточные проекты позволяют определить конкретные направления развития законодательства в части регулирования технологии блокчейн.

Для более детального понимания целесообразно рассмотреть некоторые из обозначенных проектов, которые наиболее тесно связаны именно с банковской деятельностью.

Одним из проектов является проект KYC (KnowYourCustomer), обусловленный действующим банковским принципом «знай своего клиента». В соответствии с международными требованиями и требованиями отечественного законодательства кредитные организации обязаны идентифицировать клиента перед совершением до приема его на обслуживание. Такая обязанность прямо закреплена Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

На сегодняшний день исполнение обязанности по идентификации требует от банков значительных трудозатрат, что, тем не менее, не исключает риска отсутствия необходимой информации (невозможности ее установления), для предотвращения мошеннических транзакций. В рамках проекта KYC предполагается автоматизированный обмен информацией о предполагаемых клиентах между участниками системы «Мастерчейн». То есть, после первичного предоставления сведений в один из банков, такие сведения подлежат хэшированию и загрузке в общий пул сведений. При последующем обращении лица, сведения о котором находятся в указанном пуле, в банк, участвующий в системе, и после получения указанным банком согласия на обработку персональных данных, идентификация будет произведена на основе уже имеющихся в системе сведений.

В то же время, необходимо отметить неоднозначность указанного проекта в контексте идентификации в рамках требований законодательства о противодействии легализации (отмыванию) денежных средств, полученных преступным путем. В частности, из норм статьи 7 вышеуказанного Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» следует, что банки обязаны проводить мероприятия по идентификации клиентов самостоятельно. В отдельных случаях проведение идентификации может быть поручено иной кредитной организации, однако перечень таких ситуаций жестко определен законодательством – проведение идентификации или упрощенной идентификации клиента-физического лица в целях осуществления перевода денежных средств без открытия банковского счета, в том числе электронных денежных средств, а также предоставления указанному клиенту - физическому лицу электронного средства платежа.

Учитывая изложенное, представляется, что рассматриваемый проект KYC на сегодняшний день, без внесения изменений в действующее законодательство, не может расцениваться как полноценный инструмент для повышения эффективности деятельности банков при процедуре идентификации клиентов, но, в то же время, может использоваться в качестве дополнительного источника проверки сведений о клиенте в рамках реализации правил внутреннего контроля кредитной организации.

Другим значимым проектом является проект «Цифровой аккредитив», который наиболее тесно связан с непосредственно осуществлением расчетов.

В соответствии с п. 6.1 Положения Банка России от 19.06.2012 № 383-П О правилах осуществления перевода денежных средств при расчетах по аккредитиву банк,

действующий по распоряжению плательщика об открытии аккредитива и в соответствии с его указаниями (далее - банк-эмитент), обязуется осуществить перевод денежных средств получателю средств при условии представления документов, предусмотренных аккредитивом и подтверждающих выполнение его условий (далее - исполнение аккредитива), либо предоставляет полномочие другому банку (далее - исполняющему банку) на исполнение аккредитива.

Фактически, цифровой аккредитив представляет собой один из видов смарт-контрактов. Смарт-контракты это, по сути, специальные фрагменты кода, с помощью которых автоматизируется сообщения в системе блокчейн. При этом такие контракты технически используют логику «если это, тогда – то». Процесс функционирования умных контрактов не предполагает какое-либо вовлечение людей. Это означает, что эти контракты децентрализованы, что позволяет им функционировать без посредников и регуляторов в виде третьих лиц. Умные контракты не написаны в соответствии с юридическими формулировками, но так как это компьютерные программы, то они подчиняются жестким правилам.

Сами разработчики оценивают проект как переходную схему от традиционного способа ведения бизнеса к бизнесу на основе блокчейна. Предполагается, что в будущем смарт-контракты смогут заключаться между контрагентами без привлечения посредников, в том числе, в лице банков, в результате чего ценность аккредитива как способа расчета сильно снизится.

В то же время, на сегодняшний день системы блокчейн внедряются, главным образом, в банках, в результате чего можно утверждать, что проект является крайне перспективным для банков, так как, помимо прочего, на сегодняшний день является одним из немногих проектов на основе блокчейн, предполагающих непосредственно совершение расчетов, что, в конечном счете, может явиться индикатором будущей эффективности на рынке цифровых банковских услуг.

Для дальнейшего развития технологии блокчейн и ее успешного внедрения в банковскую сферу, потенциально, позволит осуществлять межбанковские расчеты, переводы между клиентами разных банков и т.д. Фактически, блокчейн может стать гораздо более безопасным и универсальным аналогом действующей системы расчетов SWIFT. Для подобного стремительного развития необходимо совершенствование законодательства в указанном направлении.

Полномасштабное внедрение технологии блокчейн, безусловно, крайне затратный процесс во всех отношениях и, вероятнее всего, может растянуться на десятилетие. В то же время, с точки зрения правового регулирования крайне важно уже сейчас установить вектор законодательного развития и установить базовые принципы регулирования, которые позволят участникам банковского сектора опробовать систему блокчейн с минимальными правовыми рисками, в том числе, посредством создания единых информационных систем.

В этой связи принятие профильного федерального закона, как это предполагается на сегодняшний день (Законопроект «О цифровых финансовых активах») не разрешит сложившейся ситуации, но наоборот усложнит последующие попытки регулирования системы блокчейн, особенно учитывая, что законопроект направлен, прежде всего, на регулирование статуса криптовалют.

Представляется, что отправной точкой для начала законодательных изменений должны стать изменения в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» отдельный ряд норм, которые бы предусматривали существование информационных систем на базе блокчейн и, предпочтительнее, определить их общую классификацию, например, публичные системы с общим доступом, публичные системы с закрытым доступом, частные системы. Учитывая разнообразие возможностей архитектурного построения систем на базе технологии блокчейн, данная классификация является максимально общей и может не включать в себя большое количество типов систем (в том числе, в зависимости от возможных ролей участников в системе).

Одновременно, Федеральной службе безопасности в рамках своих полномочий целесообразно предусмотреть критерии и требования, предъявляемые к системам блокчейн в зависимости от их классификации и целенаправленности – очевидно, что требования к публичным или «полупубличным» системам должны быть строже, учитывая их, в том числе, социальную направленность и основополагающее значение для развития экономических отношений (к таким системам могут быть отнесены государственные системы или банковские системы).

С наиболее практической точки зрения, доработки в Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» позволят банкам увереннее использовать технологию блокчейн – в рамках изменений целесообразно предусмотреть использование системы блокчейн в качестве общего источника обмена сведениями, в

том числе, посредством внедрения в систему единых реестров лиц, в отношении которых имеются сведения о причастности к экстремизму, финансированию терроризма, реестр лиц причастных к распространению оружия массового уничтожения, внутренние банковские системы по выявлению схем по легализации доходов, полученных преступным путем. Подобные изменения станут стимулом для интегрирования технологии блокчейн во внутрибанковские процессы, что позволит участникам банковского рынка и регуляторам детальнее ознакомиться с системой, отметить преимущества и выявить недостатки, что в последующем, безусловно, отразится на эффективности более сложных проектов.

### *Список литературы*

1. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // "Российская газета", № 27, 10.02.1996.
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // "Российская газета", № 165, 29.07.2006.
3. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // "Российская газета", № 151-152, 09.08.2001.
4. Положение о правилах осуществления перевода денежных средств (утв. Банком России 19.06.2012 № 383-П) // "Вестник Банка России", № 34, 28.06.2012.
5. Децентрализованная сеть обмена и хранения информации «Мастерчейн» / Официальный сайт Ассоциации Финтех [Электронный ресурс]. URL:[http://fintechru.org/documents/Masterchain\\_whitepaper\\_11\\_08.pdf](http://fintechru.org/documents/Masterchain_whitepaper_11_08.pdf) (дата обращения: 25.03.2019).
6. Bitcoin: A Peer-to-Peer Electronic Cash System / Official website of Bitcoin Project. [Electronic resource]. URL: <https://bitcoin.org/bitcoin.pdf> (Retrieved 25.03.2019).

{social}