

**С. Н. Ткаченко, О. В. Кузьмин  
Е. В. Мельничук, Е. П. Новикова**

## **АНАЛИЗ ВОЗМОЖНОСТЕЙ ВНЕДРЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В БАНКОВСКОЙ СФЕРЕ**

84

*Проанализированы основные варианты внедрения технологии блокчейн в банковской сфере. Рассмотрены основы самой технологии, ее достоинства и ограничения. Предложен вариант внедрения технологии в виде комбинации внутреннего и внешнего блокчейнов с привлечением ресурсов регулятора в лице Центрального банка РФ.*

*The paper analyzes the main options for introducing blockchain technology in the banking sector. The foundations of the technology itself, its advantages and limitations are considered. The option of introducing technology in the form of a combination of internal and external blockchains with the involvement of the resources of the regulator represented by the Central Bank of the Russian Federation is proposed.*

**Ключевые слова:** блокчейн, банк, информационная система.

**Keywords:** blockchain, bank, information system.

### **Введение**

На сегодняшний день количество информации, которую необходимо защитить от изменений, только растет. Традиционные методы защиты информации спроектированы таким образом, что пользователи, которые не имеют прав доступа на взаимодействие с той или иной информацией, не могут получить к ней доступ. Это достигается путем разграничения прав доступа между категориями пользователей. Подобный метод защиты не является надежным, поскольку у ряда лиц (администраторов) имеется прямой доступ к данным, что может повлечь за собой несанкционированные изменения информации.

Особенностью технологии блокчейн является однозначность и неизменяемость хранимой и/или передаваемой информации. Данные характеристики призваны обеспечить безопасность хранимой информации, что должно привести к повсеместному внедрению блокчейна и исключению необходимости привлекать различных посредников, обеспечивающих неизменность данных. Примерами таких посредников могут выступать нотариальные конторы, заверяющие сделки или подтверждающие идентичность документов.

Термин «блокчейн» связан прежде всего с криптовалютами. Однако суть технологии выходит далеко за пределы электронных платежных систем.

Цель данной работы — рассмотрение некоторых аспектов применения технологии блокчейн в банковской сфере.



## Основы технологии блокчейн

Технология блокчейн пользуется популярностью в сфере финтех (FinTech), поскольку в теории позволяет сделать хранимую информацию практически достоверной.

Блокчейн – это распределенная база данных, состоящая из «цепочки блоков», где устройства хранения блоков не подключены к общему серверу [1]. В качестве данных может быть что угодно: от денежных операций до нотариальных документов. В данной сети присутствует большое количество анонимных узлов. Любой узел может добавлять информацию (факт). При этом благодаря используемым криптографическим методам всегда известно, кто именно вносит информацию. Также можно однозначно идентифицировать получателя данных, если таковой существует.

85

После первичного внесения информации она заверяется определенным количеством участников сети, после чего транзакция получает статус совершенной. В блоках блокчейна фиксируется следующая дополнительная информация:

- метка времени – определяет, когда была внесена информация в систему блокчейна;
- хэш-функция – устанавливает для каждого блока данных уникальный хэш-код.

При этом информация записывается в блокчейн в окончательном виде без возможности изменить ее в дальнейшем. Теоретически возможность внесения изменений существует, однако это потребует огромного количества вычислительных ресурсов (при условии достаточно большой распределенной сети), поэтому информация считается защищенной от изменений.

Еще одной особенностью является то, что информация может быть записана в блокчейн только после ее проверки и согласования среди участников сети. Блокчейн – это децентрализованная система. Поэтому данные не хранятся на одном сервере, а распределены на множестве узлов (нодах) сети. Вся база данных или ее части многократно повторяются на множестве узлов, что и служит защитой от случайного или преднамеренного изменения данных.

Как говорилось ранее, в основе защиты данных лежит асимметричное шифрование – криптографически стойкая хэш-функция, которая отличается от традиционной тем, что для ее расчета используются не только хранимые данные (как в традиционных базах данных или торрентах), но и другие компоненты:

- метка времени;
- хэш-код предыдущего блока;
- случайное значение.

Хэш-функция преобразует массив входных данных произвольной длины в выходную строку фиксированной длины. По этой причине блоки информации становятся взаимосвязанными, образуя цепочку



защищенных данных, для изменения которых придется менять не один блок, а весь массив информации в целом, что считается принципиально невозможным.

Случайное значение подбирается таким образом, чтобы хэш-код блока информации удовлетворял заранее сформулированному условию. Например, чтобы первые 20 битов хэш-кода были нулями. Подобное доказательство корректности данных называется «доказательство работой».

Помимо этого, существует «доказательство долей», при котором случайному участнику децентрализованной сети дается право заверки нового блока своей электронной подписью.

При попытке несанкционированного изменения блока информации во время проверки этого блока на корректность будет обнаружено несоответствие информации блока и его хэша, что выявит попытку изменить данные.

Если злоумышленник изменит не только информацию блока, но и хэш таким образом, чтобы новый хэш соответствовал новой информации, то во время проверки этого блока на корректность будет обнаружено несоответствие хэша, указанного в следующем блоке, хэшу, указанному в текущем.

В результате появляется возможность контроля за совершением транзакций в режиме реального времени: обнаружение подозрительных операций и при необходимости — их более тщательное рассмотрение специалистом, результатом которого может быть отмена транзакции.

Таким образом, информационная система, построенная на основе технологии блокчейн, обладает следующими особенностями:

- 1) данные не могут быть изменены или удалены даже администраторами системы;
- 2) информация хранится децентрализованно, в виде множества копий, поэтому при выходе из строя одного из узлов сети данные не теряются.

Недостатки блокчейна вытекают из его преимуществ. Для блокчейна требуется распределенная сеть, состоящая из большого количества компьютеров, число которых может исчисляться миллионами. Соответственно, возникает необходимость найти подобное количество вычислительных мощностей и объединить их в единую децентрализованную систему. Для бизнеса подобная задача не всегда выполнима. Для обычных пользователей требуется мотивация для подключения своего компьютера к подобной сети.

При этом количество информации, которая хранится в блокчейне, постоянно растет. Также ее невозможно удалить. Чем больше совершается транзакций, тем больше хранимой информации, которая еще и дублируется на компьютерах сети. В результате требуется постоянное увеличение места для хранения данных и рост вычислительных возможностей системы для оперативного выполнения транзакций.

В противном случае сеть может не выдержать нагрузки и все транзакции будут заморожены на продолжительное время — от нескольких



часов до нескольких дней. А учитывая взаимозависимость компьютерных сетей, влияние может носить как локальный, так и глобальный характер.

Поэтому необходимо констатировать, что для блокчейна характерны сложности с масштабированием сети и большая зависимость от вычислительных мощностей.

Различают открытые и закрытые блокчейны. В случае открытой системы возможно чтение любых данных, которые находятся в системе (пусть и в зашифрованном виде), также нет ограничений на добавление информации в блокчейн.

Закрытые (приватные) блокчейны имеют жесткие ограничения на доступ к данным и выполнению транзакций.

Также выделяют общедоступные (инклюзивные) и эксклюзивные блокчейны. В общедоступных системах любой пользователь может создавать блоки и обрабатывать транзакции. Эксклюзивные блокчейны отличаются тем, что транзакции выполняются заранее определенным кругом пользователей.

Таким образом, блокчейн как система самостоятельно регулирует себя и регламентирует взаимодействие с внешней средой и пользователями. При этом отпадает необходимость в посредниках, заверяющих подлинность или корректность действий системы. Поэтому блокчейн является саморегулируемой системой с высокой степенью доверия.

### **Использование блокчейн в банковской сфере**

Современная банковская информационная система представляет собой распределенную в пространстве систему с частично изолированными друг от друга процессами, которые обрабатываются на одном из узлов. При этом существует единое хранилище информации в виде центра обработки данных.

Операции фиксируются в виде обязательно создаваемого платежного документа. Причем подобные документы зачастую имеют бумажный вид. Так, только «Сбербанк» ежегодно тратит 2,5 млрд рублей для хранения бумажных документов. Банк хранит более 12 млрд документов в своих архивах, а все архивы занимают около 70 тыс. м<sup>2</sup>.

Применение блокчейна должно привести к дальнейшей децентрализации системы и устранению необходимости заверять каждую операцию электронной подписью или иным документом.

Поэтому одним из направлений внедрения технологии блокчейна в банковской сфере является система банковских расчетов и переводов.

Классическим вариантом внедрения блокчейна в банковские и межбанковские расчеты является использование криптовалюты в качестве единого средства расчетов. При этом роль основного регулятора должен выполнять Центральный банк России. Другими словами, криптовалюта и соответствующий ей блокчейн должны составить основу национальной платежной системы Российской Федерации.

Препятствиями для этого выступают не проработанность законодательства в этой сфере и негативная позиция ЦБ РФ. Основным направ-



лением развития ЦБ видит совершенствование системы быстрых платежей. В этом случае отпадает необходимость перехода на криптовалюту. Также не в пользу блокчейна говорит то, что на данный момент в мире отсутствуют примеры эффективного и безопасного внедрения криптовалюты в национальную платежную систему.

Еще одним препятствием подобного внедрения является необходимость майнинга данной криптовалюты, за который должен будет отвечать ЦБ РФ.

Теоретически возможно сделать множество криптовалют, которые будут наработываться различными банками, то есть появится множество автономных криптовалют и блокчейнов, связанных с финансовыми организациями. При этом роль основного регулятора останется за ЦБ РФ. В этом случае возникает необходимость обмена криптовалюты одного банка на соответствующую «монету» другой финансовой организации. По сути это похоже на межбанковскую биржу криптовалют.

Для данного случая возможности регулирования еще затруднительнее первых. Становится непонятно, каким образом привязать курс отдельных криптовалют к национальной денежной единице, каким образом осуществлять коррекцию курсов валют и контролировать их движение за пределы Российской Федерации.

Таким образом, подобные варианты внедрения блокчейна не являются перспективными по следующим причинам:

- трудности перехода на новые технологии вычисления в децентрализованной системе по сравнению с централизованной;
- проблема колебания курсов и количества криптовалюты как в национальной системе, так и в отдельных банках;
- уязвимость криптозащиты перед злоумышленниками на уровне как отдельных финансовых организаций, так и криптовалютных бирж;
- зависимость скорости транзакций от оборудования и состояния сети;
- отсутствие нормативно-правовой базы этой области на территории Российской Федерации.

Альтернативой рассмотренного выше способа внедрения блокчейна в банковской сфере является введение автономных систем в финансовых организациях. В этом случае блокчейн выполняет роль заверяющей стороны и «хранителя» всех операций. Соответственно, история всех расчетов становится неизменной и сохраняется при помощи децентрализованной системы внутри банка.

Однако в этом случае возникают опасения со стороны рядовых клиентов банка, которые понимают, что в случае внутреннего банковского блокчейна возможна «атака 51 %». По сути, мы получаем ту же самую уязвимость, что и в случае со скомпрометированным системным администратором. Чтобы этого избежать, можно использовать открытую межбанковскую систему, также построенную на блокчейне.

Тогда неизменность и достоверность хранимой информации внутри банка подтверждается стабильностью и устойчивостью открытой системы, которая поддерживается независимыми друг от друга финан-



совыми организациями. Также весьма полезно будет привлечение банковского регулятора к непосредственному построению данной открытой сети. Если количество вычислительных мощностей Центрального банка в ней будет превышать 51 %, то система будет гарантированно стабильной и защищенной от банковского сговора.

Подобная связка открытого и закрытого блокчейна не только гарантирует «чистоту» операций со стороны банков, но и защищает данные от изменений злоумышленниками. В этом случае им требуется преодолеть механизмы консенсуса как для внутреннего (эксклюзивного) блокчейна, так и для внешнего (открытого), что является достоинством данного подхода.

### Выводы

В работе была рассмотрена сущность технологии блокчейна и ее основные виды. Проанализированы достоинства и недостатки ряда способов внедрения блокчейна в банковской сфере. Показана нецелесообразность использования криптовалюты как основы блокчейна в финансовых организациях Российской Федерации. Наиболее перспективным способом использования технологии блокчейн является комбинация внутреннего и внешнего блокчейнов с привлечением ресурсов регулятора в лице ЦБ РФ. В этом случае становится возможным обеспечить высокий уровень устойчивости системы перед случайными ошибками и действиями злоумышленников.

### Список литературы

1. Федотова В. В., Емельянов Б. Г., Типнер Л. М. Понятие блокчейн и возможности его использования // European Science. 2018. №1 (33). URL: <https://cyberleninka.ru/article/n/ponyatie-blokcheyn-i-vozmozhnosti-ego-ispolzovaniya> (дата обращения: 31.08.2019).

### Об авторах

Сергей Николаевич Ткаченко — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: tkasergey@yandex.ru

Олег Валентинович Кузьмин — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: OKuzmin@kantiana.ru

Евгений Михайлович Мельничук — ассист., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: emelnichuk39@gmail.com

Екатерина Петровна Новикова — доц., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: ENovikova@kantiana.ru



### **The authors**

Dr Sergey N. Tkachenko, Associate Professor, I. Kant Baltic Federal University, Russia.

E-mail: [tkasergey@yandex.ru](mailto:tkasergey@yandex.ru).

Oleg V. Kuzmin, Assistant Professor, I. Kant Baltic Federal University, Russia.

E-mail: [OKuzmin@kantiana.ru](mailto:OKuzmin@kantiana.ru)

Evgeni M. Melnichuk, Assistant, I. Kant Baltic Federal University, Russia.

E-mail: [emelnichuk39@gmail.com](mailto:emelnichuk39@gmail.com)

Ekaterina P. Novikova, Associate Professor, I. Kant Baltic Federal University, Russia.

E-mail: [ENovikova@kantiana.ru](mailto:ENovikova@kantiana.ru)