**СИДОРОВ Д. П., КАМАЕВА А. А.**

# ПРОБЛЕМЫ ВНЕДРЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН

**Аннотация.** Одной из наиболее обсуждаемых информационных технологий последних лет является блокчейн. В большинстве публикаций рассматривается только одна сторона данной технологии, а именно ее преимущества по сравнению с классическими решениями. С другой стороны, блокчейн обладает множеством недостатков, препятствующих его практическому внедрению. В статье систематизированы ограничения и недостатки блокчейна, проанализированы возможные пути их преодоления.

**Ключевые слова:** информационные технологии, блокчейн, криптовалюта, биткойн.

**SIDOROV D. P., KAMAEVA A. A.**

# PROBLEMS OF INTRODUCTION OF BLOCKCHAIN TECHNOLOGY

**Abstract.** The blockchain is one of the most discussed information technologies of the recent years. Most publications consider only one side of this technology, namely its advantages over classical solutions. On the other hand, the blockchain has many disadvantages that prevent its practical implementation. The article presents an overview of the limitations and disadvantages of blockchain. The author analyzes some possible ways to overcome them.

**Keywords:** information technologies, blockchain, cryptocurrency, bitcoin.

Впервые технология блокчейн (англ. *blockchain*) была описана группой исследователей в 1991 году [1]. Ее возникновение напрямую связано с развитием Интернета и появлением электронных денег. Целью технологии было создание децентрализованной платежной системы, которая позволяла бы пользователям пересылать друг другу средства в атмосфере полного недоверия. Однако в то время основная масса пользователей не обладала скоростным доступом в Интернет и накопителями достаточной емкости, позволяющими реализовать идеи, заложенные в блокчейн.

Практическую реализацию технология блокчейн получила только в 2008 году, когда неизвестный пользователь под псевдонимом Сатоши Накамото (англ. *Satoshi Nakamoto*) опубликовал техническое описание своего протокола криптовалюты и создал первую версию программного обеспечения, в котором этот протокол был реализован [2]. 3 января 2009 года в новой сети, получившей название «Биткойн» (англ. Bitcoin), были сгенерированы первые блоки. Данная сеть позволяла пользователям осуществлять переводы биткойнов друг другу без участия стороннего посредника, при этом само слово «биткойн» стало употребляться не только как название самой системы, но и как название денежной единицы. На сегодняшний

день именно криптовалюты являются наиболее известным, значимым и распространенным примером использования блокчейн-технологии [3; 4].

Описание принципов функционирования технологии блокчейн с разной степенью детализации можно найти, например, в [5–7]. Резюмируя приведенную в указанных источниках информацию, базовые принципы блокчейна можно определить следующим образом.

Основной задачей технологии является хранение информации в цифровом формате, исключая возможность подделки данных. Механизм работы блокчейна основан на децентрализованной цепочке равнозначных блоков, каждый из которых содержит три элемента: данные блока, хэш блока и хэш предыдущего блока. Хэш блока – это уникальный код, который присваивается блоку с целью его последующей идентификации. Если кто-то меняет данные блока, его хэш меняется. Уличить подмену данных можно с помощью хэша предыдущего блока, который записан в следующем блоке. Несовпадение кодов указывает на замену данных в предыдущем блоке. Изменение одного блока делает все следующие за ним блоки недействительными.

В широком смысле, под термином блокчейн (цепочка блоков) понимают следующее: это полностью распределенная пиринговая система журналов учета, использующая программный модуль, реализующий алгоритм, который обрабатывает информационное содержимое упорядоченных взаимосвязанных блоков данных как единое целое с помощью криптографических технологий и технологий защиты данных для обеспечения и поддержки целостности этой системы [5].

Блокчейн позволяет автоматизировать транзакции, не привлекая при этом третью сторону. В системе нет центрального руководства, проверкой транзакций занимается особая категория пользователей, называемая майнерами. Майнеры подтверждают подлинность совершенных транзакций и формируют из них блоки, которые выстраиваются в цепочки. В отсутствии посредников кроется основное преимущество технологии. В настоящий момент все операции с деньгами, документами и прочими данными требуют наличия посредников, проверяющих подлинность проведенных операций. В блокчейне же транзакции проверяются и подтверждаются участниками системы. Программный код сети доступен всем, и любой может посмотреть данные по операциям транзакций.

В зависимости от цели применения технологии, блокчейн-блоки могут содержать самые разные данные. Например, блокчейн может применяться для хранения медицинских записей, создания цифрового нотариуса, сбора налогов, а также в других сферах, требующих учёта взаимодействия больших групп людей. Что касается криптовалют, блоки содержат

информацию о финансовых транзакциях: сумму и дату перевода, а также публичную часть идентификаторов участников сделки [6–8].

Преимуществам технологии блокчейн и возможным областям ее практического применения в настоящее время посвящено большое количество публикаций [3; 4; 6; 8; 9]. Поэтому здесь не будем даже кратко останавливаться на освещении данных вопросов. Следует отметить, что в большинстве публикаций, посвященных блокчейну, авторы концентрируют свое внимание именно на плюсах данной технологии и лишь кратко упоминают (или вообще не упоминают), что она далеко не идеальна, что у нее есть и минусы. Наиболее оптимистично настроенные эксперты предполагают, что эта технология – одно из самых важных изобретений человечества после создания всемирной сети Интернет и что скоро абсолютно все будет работать на блокчейне.

Когда заходит речь о перспективах применения блокчейна в той или иной практической области, то зачастую рассматриваются идеальные условия функционирования системы без учета влияния различных факторов, существующих в объективной реальности: накладные расходы, связанные с эксплуатацией оборудования; юридические аспекты; человеческий фактор.

Например, рассмотрим вопрос о безопасности использования технологии блокчейн в секторе криптовалют. Она обеспечивает высокий уровень защиты в сети, делая транзакции анонимными, но это одновременно создает риски для использования криптовалют в преступных целях [10]. Кроме того, технологии, лежащие в основе функционирования криптовалют, как и любые информационные системы подвержены различного рода уязвимостям.

Самым слабым в цепочке обращения криптовалют является звено, в котором криптовалюты обмениваются на традиционные деньги. Так как это происходит на вновь созданных нерегулируемых биржах, то они часто становятся объектом хакерских атак. Ярким примером проблемы безопасности криптовалют является история биржи Coincheck в Японии, которая была взломана мошенниками, в результате чего были похищены 520 млн. токенов NEM с потерями для биржи на сумму около $440 млн. Хакеры воспользовались уязвимостью IT-систем и с помощью вируса украли ключи шифрования кошельков пользователей. Эти ключи были выложены на различных сайтах в «даркнете» (DarkNet) [4].

Существуют и другие ловушки на рынке криптовалют. Например, в связи с быстрыми темпами появления новых криптобирж, становится сложно определить их исторические показатели и протестировать их на благонадежность. Появляются «серые» биржи, которые в

любой момент могут приостановить свою деятельность, заранее выведя активы, как произошло в случае с японской биржей Mt. Gox в феврале 2014 года [4].

Для правительств многих стран наиболее важной проблемой безопасности обращения криптовалют является их использование в целях отмывания денег или финансирования терроризма. Японское правительство, министры финансов и главы центральных банков Франции и Германии предлагают сделать регулирование криптовалют международным с целью предотвращения отмывания денег посредством виртуальных валют. МВФ также придерживается точки зрения о необходимости регулирования рынка цифровых валют.

Таким образом блокчейн не является абсолютно совершенной технологией и не обходится без некоторых ограничений. Систематизируем основные ограничения технологии блокчейна и причины, по которым эти ограничения создают серьезные затруднения для коммерческого применения этой технологии.

Рассмотрим технические ограничения блокчейна.

1. **Недостаточная секретность.** Блокчейн-система является полностью распределенным пиринговым реестром, обслуживающим полную хронологию данных транзакций. Все подробности транзакций, такие как передаваемые объекты и их количество, учетные записи, участвующие в передаче, и время передачи, доступны всем. Это необходимо для того, чтобы каждый член системы получил возможность определить и подтвердить право владения, а также проверить новую транзакцию (например, для обнаружения атаки типа двойное расходование). Таким образом, недостаточная секретность операций является неотъемлемым составным элементом блокчейн-системы. Без такого уровня открытости блокчейн-система не смогла бы выполнять свои функции. Но такой уровень открытости часто становится ограничивающим фактором для применения в приложениях, которые требуют большей секретности.

2. **Модель защиты.** Технология блокчейна использует асимметричную криптографию для идентификации и аутентификации пользователей, а также для авторизации транзакций. Номера учетных записей в блокчейн-системе в действительности являются открытыми криптографическими ключами. Только владелец соответствующего закрытого (секретного) ключа может получить доступ к объектам собственности, принадлежащим конкретной учетной записи. Только те данные транзакции, которые содержат цифровую подпись, созданную с помощью соответствующего секретного ключа, являются корректными и могут осуществить передачу объектов собственности из одной учетной записи в другую. Секретный ключ (private key) – это единственный инструмент защиты, позволяющий выполнить авторизацию законного владельца. После того как

секретный ключ учетной записи получает постороннее лицо преднамеренно, случайно, по ошибке или в результате перехвата данных, такая учетная запись уже не является защищенной.

3. **Ограниченная масштабируемость.** Блокчейн – это пиринговая система, ориентированная на достижение двух целей: с одной стороны, она позволяет каждому добавлять новые транзакции в совместно обслуживаемую хронологию транзакций, с другой – она обеспечивает защищенность хронологии данных транзакций от изменений и подделок. Блокчейн-система соблюдает баланс между обеими целями, используя неизменяемую структуру данных с возможностью только добавления, которая требует решения хэш-головоломки при каждой операции добавления нового блока. Решение хэш-головоломки требует значительных затрат времени, поэтому любая попытка изменения хронологии транзакций будет связана с неприемлемо большими накладными расходами. К сожалению, за такое средство защиты приходится платить снижением скорости обработки данных, следствием чего является ограниченная масштабируемость системы. Эта характеристика блокчейн-системы считается серьезным препятствием для использования ее в тех случаях, когда требуются высокая скорость обработки данных, высокая масштабируемость и высокая пропускная способность.

4. **Высокий уровень накладных расходов.** Проблема больших накладных расходов связана с проблемой ограниченной масштабируемости. Решение хэш-головоломки или подтверждение выполненной работы преднамеренно сделано чрезвычайно трудоемким и затратным в плане объема вычислений. Это средство защиты, которое делает хронологию данных транзакций практически не изменяемой. Затраты на вычисления могут быть отображены в различных единицах измерения, например в количестве вычислительных циклов, в затраченном времени, в единицах израсходованной электроэнергии или в денежном выражении. Но результат будет одним и тем же: подтверждение выполненной работы требует больших затрат. Следовательно, вся блокчейн-система связана с накладными расходами. Подавляющее большинство этих накладных расходов зависит от уровня сложности хэш-головоломок.

5. **Скрытая централизация.** Обязательность решения хэш-головоломки для каждого блока, добавляемого в структуру данных блокчейна, и правила распределенных поощрений за вклад в поддержку целостности системы неизбежно приводят к конкуренции между членами системы. Обладатели необходимых финансовых ресурсов вкладывают деньги в специализированные аппаратные средства, которые позволяют решать хэш-головоломки, тем самым внося полезный вклад в систему. С другой стороны, рискованные действия по

проверке и добавлению новых данных транзакций становятся невыгодными для тех, кто не имеет доступа к специализированной аппаратуре, следовательно, такие пользователи вынуждены отказываться от предоставления своих вычислительных ресурсов системе. В результате предположительно большая и разнородная группа равноправных партнеров, совместно поддерживающая целостность системы, в конечном итоге становится очень маленькой группой объектов, каждый из которых обладает огромной вычислительной мощностью в форме специализированных аппаратных средств. Эта оставшаяся группа партнеров образует своеобразную монополию, в которой ответственность за поддержку целостности системы разделена между немногими членами группы.

6. **Недостаточная гибкость.** Блокчейн-система – это сложная техническая конструкция, которая сформирована на основе разнообразных концепций и протоколов, оптимизированных и адаптированных для совместной работы. Любые изменения в этой тонко настроенной экосистеме могут быть чрезвычайно затруднительными. На самом деле не существует конкретно определенной процедуры изменения или обновления основных компонентов блокчейн-системы, после того как она начала свою работу. Это неявно обусловливает долгий срок сопровождения технологий, на основе которых сформирована технология блокчейна. Например, криптографические процедуры должны быть корректными на протяжении всего жизненного цикла блокчейн-системы, то есть в перспективе – в течение десятков и даже сотен лет. То же самое относится и к алгоритму блокчейна, и к методикам разрешения конфликтов. Кроме того, определенные проблемы для разработчиков блокчейн-системы связаны с ее неизменяемостью, поэтому трудно исправлять ошибки и вносить усовершенствования в протокол блокчейна. Эти характеристики делают весь комплект (стек) технологий блокчейна менее гибким, чем другие технологии.

7. **Критический размер.** Сопротивляемость различным манипуляциям и вытекающая из этого степень доверительности к совместно обслуживаемой хронологии данных транзакций основаны на предположении, что основные вычислительные мощности системы управляются честными узлами. Тем не менее в маленьких пиринговых системах с ограниченной вычислительной мощностью это управляющее большинство может оставаться весьма незначительным (в абсолютном выражении), что, в свою очередь, может создавать потенциальную возможность для проведения атак типа «51 процент». Эта проблема особенно опасна для криптовалют с низкой рыночной капитализацией и небольшим количеством пользователей-участников. Таким образом, любая блокчейн-система требует критической массы честных узлов для поддержки и обеспечения сопротивляемости атакам с применением значительных вычислительных мощностей. Достижение критического размера,

при котором атаки типа «51 процент» становятся невозможными, представляет собой очень трудную задачу, с необходимостью решения которой неизбежно сталкивается каждая новая блокчейн-система.

Существуют нетехнические ограничения блокчейна.

1. **Недоверие с юридической точки зрения.** Блокчейн – это технология, которая предоставляет пользователям возможность управления и передачи прав владения собственностью в открытой и полностью распределенной пиринговой системе. Способ, которым независимые равноправные партнеры совместно управляют правами владения собственностью с помощью распределенного согласования, поставил вопросы, касающиеся законности последовательностей транзакций, выполняемых и управляемых в блокчейн-системе. Вопросы, относящиеся к юридической правомочности и приемлемости с точки зрения законодательства транзакций, выполняемых в блокчейн-системе, должны обсуждаться вне зависимости от безопасности, защищенности и сложности соответствующей технологии. Это вопрос включения новой методики управления правами владения собственностью в существующую систему законодательства. Те, кто застал времена появления и начального развития Интернета, могут заметить сходство между юридическим статусом блокчейна в наши дни и недоверием с точки зрения законодательства к интернет-коммерции в 1990-е годы.

2. **Недоверие со стороны пользователей.** Недоверие со стороны пользователей, их предвзятое отношение является еще одним ограничением, которое нельзя недооценивать. Открытый (общедоступный) юридический статус блокчейн-системы вызывает чувство неуверенности у пользователей, в свою очередь, снижая их заинтересованность в использовании этой системы. Дополнительным фактором, влияющим на доверительное отношение пользователей, является уровень их знаний и образования. Не следует ожидать, что клиенты будут пользоваться блокчейн-системой и полностью доверять ей, если им непонятны основные принципы ее функционирования.

Подводя итог всему вышесказанному, можно сделать вывод о том, что технические и нетехнические ограничения нужно рассматривать как главные препятствия для применения технологии блокчейна в реальных приложениях. Способы преодоления конкретных ограничений всегда были и остаются предметом интенсивных исследований и перспективных разработок. Подробное обсуждение этих исследований не относится к тематике данной статьи. Тем не менее, кратко остановимся на способах преодоления ограничений технологии блокчейна.

Преодоление технических ограничений технологии блокчейна может потребовать вмешательства во все компоненты и на всех технических уровнях. Одна из главных трудностей в процессе преодоления технических ограничений технологии блокчейна – различие между усовершенствованием этой технологии и изменением ее основ.

Нетехнические ограничения технологии блокчейна могут рассматриваться как социальные, экономические, юридические и психологические аспекты перехода к новой технологии. Образовательные и законодательные инициативы могут стать дополнительными средствами для перехода к использованию блокчейна. Пример Интернета и электронной коммерции уже показал, что требуется определенное время для ответа на вопросы, связанные с законодательством, которые возникают вместе с новыми технологиями, а кроме того, время также требуется для того, чтобы пользователи поняли новые технологии, стали им доверять и применять. Тот же пример Интернета и электронной коммерции также показал, что образовательные инициативы, направленные на изучение функциональности новых технологий, увеличивают степень доверия к ним, способствуют их распространению среди пользователей и решению юридических проблем.

ЛИТЕРАТУРА

1. Haber S., Stornetta W.S. How to time-stamp a digital document // Journal of Cryptology. – January 1991. – Volume 3, Issue 2. – P. 99–111.

2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf (дата обращения 06.05.2019).

3. Винья П., Кейси М. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. – М.: Манн, Иванов и Фербер, 2017. – 432 с.

4. Соколов В. Н., Иванова К. С., Уварова П. А. Блокчейн и криптовалюты: обзор трендов и перспектив [Электронный ресурс] // Международный дискуссионный клуб «Валдай». – 2018. – Режим доступа: http://ru.valdaiclub.com/files/21191/ (дата обращения 06.05.2019).

5. Дрешер Д. Основы блокчейна: вводный курс для начинающих в 25 небольших главах. – М.: ДМК Пресс, 2018. – 312 с.

6. Лелу Л. Блокчейн от А до Я. Все о технологии десятилетия. – М.: Эксмо, 2018. – 256 с.

7. Антонопулос А. Осваиваем биткойн. Программирование блокчейна. – М.: ДМК Пресс, 2018. – 428 с.

8. Свон М. Блокчейн: Схема новой экономики. – М.: Олимп-Бизнес, 2017. – 240 с.

9. Равал С. Децентрализованные приложения. Технология Blockchain в действии. – СПб.: Питер, 2017. – 240 с.
10. Цой В. В., Царев Е. О., Домбровский Ю. Е. Обеспечение безопасности при использовании криптовалюты // Банковское дело. – 2017. – № 11. – С. 4–8.