



Экономический и Социальный Совет

Distr.: General
17 January 2019
Russian
Original: English

Европейская экономическая комиссия

Исполнительный комитет

Центр Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям

Двадцать пятая сессия

Женева, 8–9 апреля 2019 года

Пункт 7 с) предварительной повестки дня

**Рекомендации и стандарты: другие информационные
продукты для принятия к сведению**

Белая книга по обзору применения технологии блокчейн в сфере торговли

Ознакомление с использованием технологии блокчейн в сфере упрощения процедур торговли

Резюме

Технология блокчейн и технология распределенного реестра (DLT) в целом могут значительно способствовать укреплению доверия к международным торговым операциям. В стремлении сформировать общее понимание и заложить основы для всей будущей работы Центра Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН) по данной теме в настоящей Белой книге описываются основные аспекты технологии блокчейн и ее функционирования. В заключительной части документа содержатся руководящие принципы, позволяющие определить, в каких случаях применение технологии блокчейн для обработки транзакции целесообразно, а в каких – нет.

Бюро СЕФАКТ ООН представляет документ ECE/TRADE/C/CEFACT/2019/9 двадцать пятой пленарной сессии для принятия к сведению.



I. Ознакомление с использованием технологии блокчейн в сфере упрощения процедур торговли

A. Введение

1. В рамках проекта СЕФАКТ ООН, посвященного белым книгам по технологии блокчейн, были подготовлены две белые книги. В первой опубликованной Белой книге (ECE/TRADE/C/CEFACT/2019/8) рассматривается вопрос о том, как применение технологии блокчейн влияет на работу СЕФАКТ ООН в области технических стандартов. В настоящей, второй Белой книге, рассматривается вопрос о том, как технология блокчейн может быть использована для упрощения процедур торговли и связанных с ними бизнес-процессов.

2. Как будет видно из нижеследующего текста, в настоящем документе используется термин «блокчейн», хотя его использование перемежается с использованием термина «технология распределенного реестра».

3. В основе технологии блокчейн лежит принципиально новый подход к использованию криптографии, и то пристальное внимание, которое привлекает к себе эта технология, обусловлено ее характеристиками, включающими в себя:

- возможность создания постоянных записей данных (т. е. таких, которые невозможно изменить или удалить);
- возможность определять время и происхождение каждой сделанной в блокчейне записи;
- наличие у всех участников доступа ко всем данным блокчейна;
- гарантированное выполнение смарт-контрактов (программ), которые запускаются автоматически при соблюдении ряда согласованных условий.

4. Для международных производственно-сбытовых цепочек характерны потоки товаров и связанных с ними данных. Эти потоки увязаны с движением соответствующих им финансовых средств, отражающим транзакционный характер производственно-сбытовых цепочек. Движение средств, как правило, привязано к конкретным событиям в производственно-сбытовой цепочке и осуществляется в электронном виде, благодаря чему для его обработки вполне может применяться технология блокчейн. Товары поступают от экспортера к импортеру в обмен на финансовые средства, движение которых осуществляется в противоположном направлении. Поток товаров и средств сопровождается идущим в обоих направлениях потоком данных в виде, в частности, счетов-фактур, извещений об отгрузке, коносаментов, сертификатов происхождения и деклараций на ввоз/вывоз, подаваемых в регулирующие органы.

5. Из этого описания становится понятен интерес СЕФАКТ ООН к технологии блокчейн. Начиная с 1960-х годов СЕФАКТ ООН и его предшественники разрабатывают рекомендации и стандарты в целях содействия упрощению процедур торговли. После того, как в 1980-х годах был внедрен стандарт ЭДИФАКТ ООН¹, СЕФАКТ ООН начал также заниматься разработкой и поддержанием стандартов, направленных на упрощение процедур торговли путем совершенствования потоков данных, связанных с торговыми операциями.

6. Описанные выше три потока (товаров, данных и финансовых средств) опираются на наличие определенного уровня доверия. Практически все действия и операции по обмену данными в области международной торговли зависят от наличия или отсутствия доверия, в том числе доверия в отношении:

¹ Правила Организации Объединенных Наций для электронного обмена данными в управлении, торговле и на транспорте (ЭДИФАКТ ООН) представляют собой стандарт, который в настоящее время широко используется в международных перевозках, логистике и в других областях.

- происхождения и подлинности товаров;
- стоимости товаров, заявленной для целей страхования, уплаты пошлин и оплаты товаров;
- обещаний произвести платеж;
- сохранности товаров во время транспортировки (т. е. целостности упаковки, состояния транспортного средства и контейнеров и т. д.);
- целостности информации, используемой регулирующими органами для оценки рисков, которой определяется порядок проведения проверок и получения разрешений;
- торговых компаний и поставщиков услуг, участвующих в торговой сделке.

7. Уровень доверия между хозяйствующими субъектами влияет на то, какие технологии необходимы для достижения желаемого уровня надежности электронного обмена. В случае высокого уровня доверия между партнерами уместно использование методов удостоверения подлинности, которые характеризуются более низким уровнем надежности. В тех случаях, когда такое доверие между торговыми партнерами отсутствует, необходимы методы удостоверения подлинности с более высокой степенью надежности. Уровень доверия (или недоверия) в значительной степени по-прежнему поддерживается за счет использования бумажных документов, рукописных подписей, страховых платежей, депонирования средств и других услуг, оказываемых доверительными третьими сторонами.

8. Технология блокчейн представляет собой разновидность технологии распределенного реестра (DLT), которая позволяет использовать методы удостоверения подлинности, характеризующиеся весьма высоким уровнем надежности. Таким образом, она обладает потенциалом обеспечить значительно более высокий уровень доверия, о котором говорилось выше, причем зачастую с меньшими затратами и при более высоких скоростях обмена данными, чем в случае альтернативных вариантов.

9. Как DLT, так и технология блокчейн могут в значительной степени повысить уровень доверия и автоматизировать его обеспечение. В последующей части настоящего документа обсуждается только технология блокчейн при том понимании, что она является одной из разновидностей DLT.

10. Будучи координационным центром системы Организации Объединенных Наций по упрощению процедур торговли и стандартам электронных деловых операций, СЕФАКТ ООН должен задаться вопросом о том, какое влияние эта новая технология оказывает на эти две основные области его работы. В первой Белой книге (ECE/TRADE/C/CEFACT/2019/8) рассматривается влияние технологии блокчейн в области стандартов СЕФАКТ ООН по ведению электронных деловых операций, а настоящая Белая книга посвящена влиянию этой технологии на сферу упрощения процедур торговли. Был проведен анализ нескольких секторов торговли, поскольку в разных секторах имеются разные запросы в плане доверия, а с течением времени в них сформировались различные механизмы для удовлетворения этих запросов. Таким образом, проанализировать использование технологии блокчейн во всех сферах торговли не представляется возможным, несмотря на то, что все они сталкиваются с одинаковыми проблемами и испытывают одинаковые потребности. Список рассмотренных секторов приводится ниже, а с результатами анализа можно ознакомиться в документе, озаглавленном «Технология блокчейн в сфере упрощения процедур торговли: отраслевые проблемы и примеры» (ECE/TRADE/C/CEFACT/2019/INF.2). В этом документе обсуждаются следующие горизонтальные и вертикальные аспекты:

- горизонтальные аспекты:
 - вопросы безопасности и нормативно-правовые вопросы использования технологии блокчейн;

- вклад технологии блокчейн в достижение Целей устойчивого развития Организации Объединенных Наций (ЦУР);
- вертикальные аспекты:
 - производственно-сбытовые цепочки, отслеживаемость и блокчейн;
 - морской транспорт и блокчейн;
 - неморские виды перевозок и блокчейн;
 - торговля сельскохозяйственной продукцией и блокчейн;
 - финансовые услуги и блокчейн;
 - услуги государственных учреждений и блокчейн;
 - туризм и блокчейн;
 - музыка и изобразительное искусство и блокчейн;
 - услуги здравоохранения и блокчейн.

11. Помимо этого, с использованием формуляра, который содержится в приложении, была собрана информация о примерах использования технологии блокчейн и существующих блокчейн-решениях.

В. Последующие шаги

12. Проектная группа СЕФАКТ ООН, занимающаяся подготовкой белых книг по технологии блокчейн, провела очное совещание в ходе Форума в Ханчжоу (Китай) в октябре 2018 года. В ходе этого совещания был достигнут консенсус в отношении того, что одним из наиболее важных положительных аспектов данного проекта является предоставление тем, кто внедряет или рассматривает возможность внедрения технологии блокчейн, возможности провести предметное обсуждение преимуществ, альтернатив, проблем и возможных решений. Существует множество форумов и конференций по технологии блокчейн, однако они посвящены преимущественно криптовалютным или инвестиционным аспектам и/или не предоставляют возможностей для диалога (т. е. в основном ориентированы на распространение информации) и/или на них доминируют мнения тех, кто занимается продажами и продвижением конкретных блокчейн-решений.

13. В целях развития этой темы проектная группа предложила создать форум для обсуждения вопросов использования технологии блокчейн в международных производственно-сбытовых цепочках и включить в его сферу охвата другие передовые технологии, в частности Интернет вещей (IoT) и искусственный интеллект (AI). Этот форум мог бы оказать поддержку руководителям высшего звена, особенно в государственном управлении, ответственным за принятие решений о работе международных производственно-сбытовых цепочек. Он мог бы также помочь СЕФАКТ ООН выявить области, в которых его работа могла бы способствовать использованию этих передовых технологий в целях упрощения процедур торговли.

14. Проектная группа поддержала предложение о создании Консультативной группы по вопросам передовых технологий в области торговли и логистики², которая будет оказывать поддержку в осуществлении программы работы СЕФАКТ ООН в областях, связанных с использованием цифровых технологий для обмена торговой информацией. Ее основная задача будет заключаться в выявлении возникающих проблем стратегического характера и передовой международной практики старших должностных лиц из государственного и частного секторов, занимающихся данной темой. Одним из первых направлений деятельности этой Консультативной группы станет рассмотрение конкретных проблем, выявленных в ходе анализа по отраслям и в рамках конкретных примеров, содержащихся в настоящей Белой книге. Исходя из

² См. предлагаемые «Мандат и круг ведения Консультативной группы по вопросам передовых технологий в области торговли и логистики» (ECE/TRADE/C/CEFACT/2019/22).

результатов этой работы, Консультативная группа будет оказывать консультативную поддержку для разработки рекомендаций относительно будущей работы, а также руководящих принципов и информационных продуктов для принятия к сведению и, возможно, для утверждения СЕФАКТ ООН.

II. Что такое блокчейн и какие бывают типы блокчейнов

A. История и общие сведения

15. Основы используемой сегодня технологии блокчейн были впервые описаны в октябре 2008 года в Белой книге, опубликованной в списке рассылки о криптографии, хотя некоторые принципы, лежащие в основе в технологии блокчейн, описывались в более ранних работах. Белая книга называлась «Биткойн: система цифровой пиринговой наличности» и была опубликована автором или группой авторов, скрывающихся под псевдонимом *Сатоси Накамото*. Любопытно, что в исходной публикации ни разу не встречался термин «блокчейн», вместо которого в ней использовались такие слова, как «цепочка» и «блоки» (которые составляют цепочку). Впервые термин «блокчейн» появился в том же списке рассылки о криптографии в ходе последующих обсуждений, связанных с исходной книгой Накамото.

16. 9 января 2009 года Сатоси Накамото выпустил версию 0.1 программного обеспечения Биткойн, в котором впервые были реализованы принципы, описанные в публикации, вышедшей в октябре 2008 года. Новая программа была размещена на сайте программного обеспечения с открытыми исходными кодами под названием SourceForge.

17. Сатоси Накамото продолжал сотрудничать с другими разработчиками программного обеспечения Биткойн до середины 2010 года. Примерно в это время он передал Гевину Андресену контроль над репозиторием исходных кодов и обновлениями, передал ряд смежных интернет-доменов другим видным членам сообщества разработчиков биткойна и покинул проект. Несмотря на многочисленные спекуляции и поиски, до сих пор никому не удалось установить личность Сатоси Накамото.

18. Другой важной вехой в развитии технологии блокчейн стало создание блокчейнов, способных выполнять небольшие компьютерные программы под названием «смарт-контракты», написанные на языках программирования, которые характеризуются полным набором возможностей в области программирования (так называемые «полные по Тьюрингу» языки программирования).

19. Благодаря смарт-контрактам блокчейны могут осуществлять набор разнообразных бизнес-функций, связанных с передачей информации и/или значений, оставляя при этом прозрачные и стабильно проверяемые информационные следы. Далее в тексте приводится более подробная информация о смарт-контрактах.

20. Первым блокчейном, в котором используются смарт-контракты, стал Ethereum («Эфириум»), созданный Виталиком Бутериным. Впервые использование смарт-контрактов на базе блокчейна было описано им в Белой книге, опубликованной в конце 2013 года. Затем, после того как ему не удалось добиться согласия по этой концепции среди сообщества разработчиков биткойна, он предложил разработку новой платформы под названием Ethereum. Эта новая сеть, запущенная 30 июля 2015 года, на сегодняшний день является самым крупным блокчейном по количеству транзакций и входит в тройку лидеров по объемам рыночной капитализации³.

³ According to <https://bitinfocharts.com/> (as of December 2018).

В. Как работает блокчейн

21. По сути, блокчейн представляет собой криптографический протокол, позволяющий отдельным сторонам добиться высокого уровня доверия к транзакциям благодаря тому, что записи в реестре его базы данных не могут быть легко фальсифицированы (т. е. после того, как данные записаны в реестр, изменить их чрезвычайно трудно). Такая неизменяемость достигается за счет сочетания ряда факторов, в том числе используемых в блокчейне криптографических алгоритмов, механизмов консенсуса/валидации и его распределенного характера. Благодаря своей неизменяемости блокчейн-системы могут играть роль независимых арбитров в процессах, которые в противном случае сопряжены с риском того, что одна из сторон не выполнит свои договорные обязательства (риск несостоятельности контрагента), а гаранты в лице третьих сторон будут стараться не вмешиваться в эти процессы и не принимать на себя часть этого риска.

22. В рамках данного документа не ставилась задача провести углубленный обзор технологии блокчейн – есть множество веб-ресурсов, которые могут помочь читателям справиться с этой задачей. Вместо этого в документе представлены основные концепции, необходимые для понимания возможностей в плане применения технологии блокчейн в международных производственно-сбытовых цепочках.

23. Для начала следует определить некоторые термины:

a) Блок: данные, которые добавляются в реестр после их проверки. После того, как блок записывается в цепочку, его невозможно изменить или удалить без замены всех последующих блоков.

b) Консенсус: его соблюдение является важной особенностью блокчейн-систем, благодаря которой пользователи узнают о том, что транзакция имела место, и могут оценить достоверность как информации внутри самой транзакции, так и информации о ней (в частности, дату/время совершения и содержимое транзакции). В открытых блокчейнах в качестве арбитра, принимающего решение о наличии консенсуса, выступает группа всех узлов, которые решили принимать участие в механизме консенсуса. В закрытых блокчейнах арбитром является консорциум, в который входят узлы, получивших разрешение на участие в механизме консенсуса. Далее в тексте содержится более подробная информация о различных способах достижения консенсуса.

c) Фиаты, или фиатные деньги: это валюты, которые поддерживаются центральным банком, например доллары, евро, иены и т. д.

d) Хэш: результат математических вычислений, произведенных с числовым представлением данных (в компьютере все данные представлены в форме чисел, которые декодируются для того, чтобы данные на экране могли быть отображены в виде слов и изображений). Этот результат характеризуется фиксированным размером и представляет собой уникальный криптографический «отпечаток» данных, с использованием которых он был получен. Хеширование является односторонней функцией; это означает, что, имея в своем распоряжении данные, можно легко проверить правильность хэша для них. Проверка осуществляется путем выполнения заранее определенных математических операций с данными, на основе которых, как предполагается, был получен хэш: если результат проверки идентичен хэшу, то и данные в обоих случаях одни и те же. Эта функция ключевая, поскольку она позволяет пользователям быстро проверить, были ли внесены какие-либо изменения. Например, добавление в тексте даже одного знака пробела или пустой строки изменит его хэш. В то же время на основе одного только хэша практически невозможно воссоздать исходные данные (т. е. совершить обратное преобразование), что и делает эту функцию односторонней.

e) **Узел:** система, в которой хранится полная копия блокчейн-реестра. В одних блокчейнах, например в Биткойне и Эфириуме, в осуществлении алгоритма консенсус могут участвовать все узлы, а в других блокчейнах – лишь некоторые из них.

f) **Цепочечная транзакция:** автоматизированная процедура, в рамках которой в результате добавления в реестр новых данных происходит создание в базе данных блокчейна блокчейн-ресурса или обновление его статуса. Примеры таких транзакций включают в себя обмен цифровыми активами или выполнение автоматизированного бизнес-процесса.

g) **Валидация:** одновременно выполняемая узлами работа, в ходе которой осуществляется проверка транзакций с использованием алгоритма консенсуса. В разных сетях могут использоваться разные алгоритмы консенсуса. Если по итогам взаимной проверки достигается консенсус, то все узлы регистрируют (записывают) в своей копии блокчейна проверенные транзакции в виде нового блока.

1. Блокчейн является одной из разновидностей технологии распределенного реестра (DLT)

24. Реестры – это перечни записей, в которых транзакции регистрируются один раз, после чего они не могут быть изменены. Это означает, что любые изменения должны регистрироваться как новые транзакции (записи в учетных реестрах). Цифровые реестры могут храниться в виде базы данных, которая называется также базой данных реестра. Каждая запись может быть прочитана многократно, но сделать ее можно только один раз. Слово «реестр» пришло из бухгалтерской отчетности, где записи, внесенные в реестр (книгу) бухгалтерского учета, не могут быть изменены. Поскольку использование хэшей обеспечивает гарантию того, что никакие из данных, содержащихся в базе данных блокчейна, никогда не подвергались изменению, такая база данных представляет собой реестр.

25. База данных блокчейн-реестра носит распределенный характер, поскольку множество ее копий хранятся в разных узлах. С помощью алгоритма консенсуса (существуют разные типы этого алгоритма) происходит скоординированное обновление многочисленных копий путем добавления к ним новых блоков данных, благодаря чему обеспечивается идентичность всех копий.

26. Таким образом, содержимое блоков данных и их последовательность в блокчейне определяются консенсусом участвующих узлов, а каждый блок содержит «отпечаток» (хэш), который может быть использован для рекурсивной проверки содержимого всех предыдущих блоков.

2. В блокчейн записываются транзакции

27. Каждый блок данных, записанный в блокчейн-реестр, содержит по крайней мере одну запись о транзакции, хотя в большинстве случаев блоки содержат множество записей о транзакциях. Простым примером транзакции может служить списание одной монеты со счета А и начисление одной монеты на счет В, хотя возможны и многие другие виды транзакций. Одни блокчейны поддерживают ограниченный набор транзакций (операций или алгоритмов), таких как эта простая двойная бухгалтерская проводка. Другие блокчейны поддерживают гораздо более широкий набор транзакций, охватывающий все разрешимые алгоритмы (т. е. полные по Тьюрингу языки программирования⁴). Для обозначения типов транзакций используются разные названия: смарт-контракты, чейнкоды, семейства транзакций или другие эквивалентные им термины. В общем виде все блокчейны поддерживают

⁴ С помощью полного по Тьюрингу языка программирования можно решить любую математическую задачу путем вычислений (при условии, что вы сможете написать на нем нужную программу). В целом это означает, что такой язык должен давать возможность осуществлять повторение или скачок при определенных заданных условиях («до тех пор, пока», «если», «когда» и «перейти к») и включать в себя способ считывания и записи данных с использованием некоторого механизма хранения (переменных значений).

разнообразные операции с данными, однако не все блокчейны поддерживают полные по Тьюрингу языки транзакций.

3. Транзакции записываются в блок, подписанный криптографической подписью

28. В блокчейнах применяются две разновидности криптографических технологий: хэш-функции и криптосистемы с открытым/закрытым ключом. Хэш-функции используются для получения неопровержимого доказательства за счет привязки каждого блока ко всей предшествующей ему цепочке. В другом контексте хэши также могут использоваться для получения доказательства валидности данных, на которые содержатся ссылки в блоках, а кроме того они применяются в алгоритмах консенсуса, связанных с доказательством выполнения работы, где хэш с определенным количеством начальных нулей играет роль «сложной задачи», которую должны решить узлы, чтобы достичь консенсуса.

29. Криптосистемы с открытым/закрытым ключом применяются для идентификации участников транзакции и контроля доступа к данным. Можно провести аналогию с электронной почтой, где открытым ключом является ваш адрес электронной почты, который может быть использован другими для отправки вам сообщений, а закрытым ключом – ваш пароль, дающий доступ к закрытой информации, т. е. к полученным вами сообщениям. Таким образом, в блокчейне открытый ключ может использоваться, например, для осуществления транзакции, в результате которой документ или платеж передается тому или иному участнику, однако доступ к документу или платежу после их отправки может получить только тот участник, у которого имеется закрытый ключ.

4. Независимые узлы должны проводить проверку блока, подписанного криптографической подписью

30. Существуют различные алгоритмы консенсуса, используемые в разных блокчейн-системах. Например, в открытом блокчейне Биткойн используются алгоритмы доказательства выполнения работы, которые позволяют майнерам возмещать свои расходы на затратные с точки зрения вычислений операции за счет комиссии, взимаемой за транзакции; эта комиссия, кроме того, является одним из способов первоначального ввода криптовалюты в обращение. В контролируемых реестрах результат процесса выработки консенсуса согласуется консорциумом узлов, которые пользуются коллективным (но не обязательно индивидуальным) доверием, что, как правило, дешевле и быстрее, чем алгоритм доказательства выполнения работы, применяемый в Биткойне. Для любых процедур консенсуса необходим механизм урегулирования споров (или снятия неопределенности) относительно вопроса о том, какой блок будет зарегистрирован следующим. В большинстве таких механизмов выбирается тот блок, который был согласован более чем 50% узлов. Более подробное описание открытых и контролируемых блокчейнов приводится ниже.

31. Природой механизма консенсуса определяются некоторые ключевые характеристики блокчейн-системы. Например, майнинг, целью которого является создание блоков, намеренно был сделан затратным. Это защищает блокчейн благодаря тому, что издержки, связанные с взятием под контроль более 50% узлов (именно такое их количество необходимо для одобрения блока и, следовательно, для манипулирования блокчейном), оказываются непомерно высокими. Чтобы компенсировать затраты майнеров, им предоставляется вознаграждение в виде некоторого количества биткойнов за каждый созданный ими блок и в виде комиссии за каждую транзакцию, записанную в блокчейн⁵. Размеры каждого блока ограничены, а стоимость транзакций определяется на свободно-рыночной основе, поэтому чем больше количество запрашиваемых транзакций, тем выше стоимость каждой из них. Это необходимое условие для работы используемой в Биткойне модели экономических операций, которая ориентирована на достижение подлинного

⁵ Биткойн спроектирован таким образом, чтобы размеры вознаграждения за майнинг с течением времени уменьшались и в конечном итоге целиком формировались за счет комиссии за транзакции.

консенсуса в условиях нерегулируемого рынка с участием потенциально анонимных и экономически грамотных операторов (т. е. операторов, которые могут похищать активы, пользуясь своей анонимностью и ничем при этом не рискуя). Имеется еще один механизм дополнительного стимулирования: если узел/майнер не принимает блок, за который проголосовали более 50% других узлов, он фактически сбрасывается с блокчейна, теряя таким образом возможность в дальнейшем зарабатывать биткойны и получать комиссионные за транзакции. Вследствие этого пропускная способность блокчейна Биткойн оказывается чрезвычайно низкой из-за издержек на создание блоков, обусловленных тем, что на подтверждение транзакций уходит в среднем десять минут. Кроме того, ввиду очень большого количества узлов и пользователей, генерирующих большие объемы данных, а также ввиду ограничений по размеру блоков хранение данных в блокчейне Биткойн оказывается не только дорогостоящим, но и неэффективным.

32. С учетом того, что информация дублируется в каждом из узлов блокчейна, хранение значительных объемов данных в блокчейне, как правило, неэффективно. Блокчейн Биткойн по-прежнему поддерживает существование массы биткойнов стоимостью в несколько миллиардов долл. США и осуществляет другие дорогостоящие транзакции, но ограничения по скорости и объему делают его непригодным для многих корпоративных приложений или для непосредственного осуществления незначительных транзакций.

33. В контролируемых реестрах баланс между пропускной способностью, эффективностью и обеспечением доверия достигается иначе. Так, поскольку контролируемые реестры имеют больше контроля в отношении выбора участников реестра, в них могут использоваться другие механизмы консенсуса, несмотря на то, что некоторые из них чуть менее надежны, чем алгоритм доказательства выполнения работы, используемый в Биткойне. Например, существуют механизмы консенсуса, в основе которых лежит объем вклада узлов в работу сети (так называемое доказательство доли владения), или механизмы, в которых консенсус подгруппы узлов проверяется более крупной группой.

34. Помимо этого, фонды, университеты и компании проводят многочисленные исследования с целью поиска и тестирования иных механизмов консенсуса. Некоторые из этих альтернативных механизмов консенсуса позволяют реестрам поддерживать осуществление сотен или даже тысяч транзакций в секунду, вместо того, чтобы создавать один новый блок в среднем один раз в десять минут, как это происходит в Биткойне. Кроме того, ведутся исследования, посвященные обслуживанию и использованию поистине гигантских баз данных, масштабы которых измеряются петабайтами.

5. После завершения проверки блок записывается в реестр

35. В случае консенсуса, наличие которого означает согласие относительно того, что блок содержит легитимные данные и что именно данный блок должен быть записан в цепочку следующим, в каждом узле согласованный блок добавляется в хранящуюся в нем копию реестра. Таким образом, каждый раз при записи нового блока во всех узлах вновь оказываются одинаковые копии реестра. Доказательством этого станет следующий записываемый блок, так как он будет содержать хэш блока, который ему предшествовал.

6. Привязка нового блока к предыдущим блокам порождает неизменяемость

36. Следует напомнить, что хэш – это односторонняя функция, которая генерирует уникальный «отпечаток» выбранных данных. Следует также учитывать, что результатом хэш-функции является «отпечаток», размер которого фиксирован, каким бы ни был объем хэшируемых данных. Поэтому по хэшу невозможно определить, содержался ли в исходных данных единичный небольшой документ или целая база данных, состоящая из нескольких миллиардов записей.

37. В каждом блоке блокчейна содержится некоторое количество данных о транзакциях и хэш предыдущего блока, размер которого всегда одинаковый,

независимо от объема данных, которые он представляет. При наличии консенсуса относительно включения нового блока в цепочку по его хэшу можно проверить предыдущий блок, а по хэшу предыдущего блока можно проверить предшествующий ему блок и так далее по всей цепочке до ее самого первого (или первичного) блока. Хэш предыдущего блока как бы привязан к последующему блоку.

38. Взлом содержимого любого блока из цепи ведет к изменению хэша этого блока, что вызывает изменение хэша блока, следующего за ним, и так далее для каждого последующего блока в цепи. В этом случае попытка взлома будет быстро выявлена любым из узлов, а алгоритмы консенсуса не допустят добавления в цепочку новых блоков, так как их хэши не будут валидными.

39. Именно благодаря этой особенности в слове «блокчейн» («цепочка блоков») присутствует слово «цепочка»: каждый блок привязан к предыдущему, и каждый блок подтверждает существование всех данных, на которые в нем содержатся ссылки, вплоть до самого первого «блока» данных, содержащегося в «цепочке».

С. Типы блокчейнов

1. Открытые реестры

40. С содержимым открытых реестров могут ознакомиться все. Кроме того, такие реестры являются бесконтрольными, поскольку любой желающий может участвовать в работе их механизмов консенсуса и воспользоваться ими, не требуя для этого разрешения и не находясь в зависимом положении от регулятора, который обеспечивает соблюдение правил поведения. Работа платформ биткойна, эфира и ряда других криптовалют, рыночная капитализация которых достигает 59 млрд долл. США⁶, организована именно таким образом, что позволяет совершать любые логически корректные транзакции между всеми участниками сети, включая анонимных и пользующихся псевдонимом участников.

41. Одно из опасений, связанных с технологией блокчейн, заключается в том, что если большая часть узлов окажется под контролем злоумышленника, то решение о наличии консенсуса может быть принято вопреки интересам других участников. В литературе по криптографии такая угроза получила название «атаки Сивиллы». Если криптовалюта на базе открытого блокчейна подвергнется успешной атаке Сивиллы, то это может привести к перераспределению активов и/или двойному расходованию с катастрофическими последствиями. Открытые блокчейн-реестры разрабатываются таким образом, чтобы их работа подчинялась правилам, не требующим вмешательства со стороны механизмов управления или регулирования для предотвращения несанкционированных транзакций, так как сами же эти механизмы могут быть использованы со злым умыслом (например, если механизм управления будет взломан третьей стороной или если доверенный орган регулирования злоупотребит им). В основе работы открытых блокчейнов лежит абсолютное доверие к их алгоритмам, и разрабатываются они так, чтобы необходимости доверять контрагентам вообще не было. Именно поэтому иногда говорят, что открытые блокчейны «не требуют доверия».

42. В открытых реестрах ради повышения устойчивости к атакам Сивиллы, как правило, приходится жертвовать другими аспектами эффективности. Кроме того, работа этих реестров зависит от прозрачности открытого реестра и прозрачности используемого им программного обеспечения с открытым исходным кодом.

2. Контролируемые/закрытые реестры

43. Как и в случае традиционных баз данных, содержимое закрытого блокчейн-реестра может быть конфиденциальной информацией, доступ к которой для отдельных пользователей и операторов узлов регулируется с помощью механизма

⁶ <https://bitinfocharts.com/> at 14:00 on 8 December 2018.

предоставления доступа с учетом функций. Аналогичным образом, закрытый блокчейн может быть сконфигурирован таким образом, чтобы ознакомиться с данными могли все желающие, а добавлять новые данные могли только назначенные узлы. В случае открытой базы данных можно добиться того же самого, используя смарт-контракты, хотя у полномочных пользователей могут возникнуть опасения в связи с повышением уровня угрозы безопасности, обусловленным тем, что любой желающий может увидеть (и попытаться взломать) эти смарт-контракты. Такая база данных может быть полезной для ведения официального учета, например, земельных сделок, выданных лицензий, сертификатов и т. д. В отличие от традиционных баз данных закрытый блокчейн-реестр является неизменяемым (т. е. содержащаяся в нем информация не может быть изменена), а для проверки транзакций в нем применяется механизм консенсуса, устанавливаемый операторами сети.

44. Технология закрытых реестров обычно применяется в тех случаях, когда предприятию необходимо, чтобы неизменяемые транзакции могли быть проверены закрытой группой узлов. Эти узлы могут действовать независимо от сторон транзакций в блокчейне и могут подвергаться надзору и управлению, осуществление которых невозможно или нежелательно в случае открытых блокчейн-систем, где получение разрешений не требуется.

45. В случае контролируемых реестров модель угроз оказывается иной, нежели в случае открытых реестров. В контролируемых реестрах операторы узлов не являются анонимными, подчиняются определенным механизмам управления и пользуются коллективным доверием пользователей. Вредоносные действия какого-либо узла или участника могут привести к их исключению из сети и блокированию их транзакций. Пользователи контролируемых реестров рассчитывают на то, что операторы вмешаются в случае совершения действий, представляющих опасность для сети, и что сами операторы совершать опасных действий не будут.

46. В контролируемых реестрах уровень безопасности и, следовательно, уверенности пользователей в неизменяемости данных, варьируют в зависимости от установленных для конкретного реестра правил, в том числе от механизма консенсуса. Из-за того, что только доверенным участникам разрешается быть операторами узлов и участвовать в верификации, контролируемые реестры могут также порождать ложное ощущение безопасности. В то же время даже пользующиеся доверием участники могут оказаться ненадежными после того, как подвергнутся взлому; контролируемые реестры также уязвимы в тех случаях, когда выходят из строя их элементы, отказ которых критичен для всей системы, а плохо протестированные смарт-контракты чреваты негативными последствиями для участников блокчейн-сети (даже если изначально не было желания нанести ущерб), в особенности если в ней отсутствуют надежные механизмы контроля.

3. Межреестровый аспект: осуществление транзакций между реестрами

47. На сегодняшний день существует множество различных блокчейнов, и в будущем их число только возрастет. Уже сейчас проведение одной транзакции от первого до последнего этапа производственно-сбытовой цепочки может быть сопряжено с записью или считыванием данных в нескольких блокчейнах. Так, экспортер может быть вынужден использовать блокчейн банка, по одному блокчейну на каждый вид перевозки, блокчейн импортера, обеспечивающий отслеживаемость, и один или несколько блокчейнов, которыми пользуются регулирующие органы. Помимо этого, нетрудно представить, что будет возрастать и потребность в информационном обмене и в осуществлении транзакций между блокчейнами (т. е. между реестрами).

48. В блокчейне могут быть размещены ссылки на данные, расположенные за его пределами. К ним относятся данные, хранящиеся в других блокчейнах, а также данные из неблокчейновых систем. Ссылки на внешние данные, которые могут использоваться в блокчейн-системах, относятся к двум обширным категориям: связанные данные и транзакции, затрагивающие разные блокчейны.

49. В связанных данных используются хэши и могут также использоваться цифровые идентификаторы и криптосистемы с открытым ключом. Такие ссылки будут рабочими при условии последовательного соблюдения правил на всем протяжении блокчейна и в системе (или системах), где хранятся связанные данные. Это означает, что чем более стандартизированным будет использование криптосистем с открытым ключом, тем проще и дешевле будет связывать данные (и то же самое можно сказать в отношении семантики, на основе которой дается определение данным). Использование единой семантики (т. е. общих определений данных) значительно упрощает интерпретацию данных из различных источников, и в этом отношении можно использовать Библиотеку ключевых компонентов СЕФАКТ ООН, которая представляет собой весьма полную библиотеку семантики, связанной с торговлей.

50. Ссылки в блокчейне, указывающие на внешние данные (также известные как «точки привязки»), также могут содержать информацию, например хэши, применяемую для доказательства существования или неизменного характера данных, на которые указывает ссылка. В этом заключается их отличие от гиперссылок или единых указателей ресурсов (URL) в Интернете, при использовании которых информация, находящаяся по тому или иному адресу, может меняться в зависимости от того, в какой момент времени к ней обращаются. Например, если вы перейдете по ссылке на веб-сайт новостного телеканала, наполнение которого по мере обновления регулярно меняется, то информация, которую вы найдете на веб-сайте завтра, может отличаться от того, что вы видите сегодня. В случае же наличия в блокчейне точки привязки ссылки на данные содержащаяся в блокчейне информация является гарантией (доказательством существования) того, что указанные данные не были изменены.

51. Помимо использования для увязывания между собой данных из двух блокчейн-систем (перекрестных ссылок на блокчейны) и использования в качестве указателя для сведений из более традиционных баз данных, которые могут быть использованы смарт-контрактом (например, для выдачи свидетельства о прохождении проверки), связанные данные могут применяться для включения в ограниченную по размерам блокчейн-систему больших данных, расположенных вне блокчейна. Вспомогательные данные могут храниться либо в открытых/общедоступных распределенных информационных системах, таких как Межпланетная файловая система (IPFS), представляющая собой открытую, контекстно-адресуемую память, в которой используются стандартные интернет-протоколы, либо в закрытых базах данных, которые доступны пользователям контролируемого реестра выборочно. Пользуясь внецепочечными или межцепочечными ссылками, операторы сети могут узнавать о существовании определенных данных, однако их доступ к ним может быть ограничен дополнительными механизмами контроля. Это может представлять интерес с точки зрения обеспечения конфиденциальности, поскольку это позволит, например, получать доступ к информации для того, чтобы, не имея сведений о возрасте человека, можно было установить, является ли он совершеннолетним, или же для того, чтобы, не имея адрес человека, узнать, проживает ли он в Лондоне.

52. Такие источники внешних данных, иногда называемые оракулами, будут подробнее рассмотрены ниже.

53. В межреестровых (затрагивающих разные блокчейны) транзакциях применяются межцепочечные ссылки и смарт-контракты (см. описание ниже), которые расположены в обоих блокчейнах и взаимодействуют между собой скоординированным образом. Эта область только зарождается, однако некоторые механизмы уже существуют и используются. Они предназначены в первую очередь для обмена значениями (т. е. цифровыми активами) между реестрами (например, межреестровый протокол Ripple и платежный протокол Lightning Network).

D. Смарт-контракты, оракулы и Интернет вещей с использованием технологии блокчейн

1. Смарт-контракты

54. Смарт-контракты – это самоисполняющиеся компьютерные программы, в которых закодирована логика деловых процессов. Их выполнение запускается при соблюдении заранее определенных условий. Иными словами, вмешательство человека (по крайней мере, напрямую) не приводит к началу их выполнения. Они могут быть весьма простыми, как, например, перевод определенной суммы активов со счета X на счет Y. В основе смарт-контрактов лежит условная модель типа «Если – то» (IFTTT), согласно которой соблюдение определенных условий приводит к выполнению некоторых действий. К таким условиям могут относиться определенные отрезки времени, заданные значения (например, стоимость каких-либо активов, в частности ценных бумаг) или конкретные события, такие как доставка клиенту заказанных товаров.

55. Смарт-контракты обладают рядом преимуществ:

- повышение уровня безопасности и предсказуемости благодаря исключению человеческого фактора и возможности умышленного или неумышленного нарушения контракта в результате действий человека;
- прозрачность, обусловленная тем, что код смарт-контракта может быть общедоступным и открытым, и тем, что любой желающий может проанализировать его и предсказать, каким образом будут осуществляться транзакции в рамках конкретного контракта;
- более простое программирование систем, которые должны принимать, сопоставлять и использовать в своих операциях данные от широкого круга участников, многие из которых могут быть неизвестны.

56. Используя понятия из повседневной жизни, можно привести следующий пример смарт-контракта:

- **Предварительное условие:** некоторое количество криптовалюты было внесено мною на депозит, а другой участник внес на депозит некоторое количество фиатных денег;
- **Условие:** если в соответствии с текущим курсом обмена обе суммы окажутся равны;
- **Действие:** то между счетами участвующих сторон будет произведен обмен валютными средствами.

57. Можно привести другой пример, связанный с арендой автомобиля: агентство, предоставляющее автомобиль в прокат, может потребовать внести через блокчейн авансовый платеж. В дальнейшем эта сумма будет разблокирована для агентства только после того, как арендатор подтвердит, что ключи от автомобиля были получены. Таким образом, с помощью смарт-контрактов можно предотвращать схемы мошенничества, связанные с применением авансовых платежей, и создавать дополнительные гарантии.

58. Так как смарт-контракты по сути являются небольшими компьютерными программами, они могут разрабатываться и адаптироваться для различных ситуаций, что делает их потенциально мощным инструментом для бизнеса.

2. Оракулы

59. Главная функция оракулов заключается в том, чтобы предоставлять смарт-контрактам на базе блокчейн безопасные и достоверные данные. После этого смарт-контракты проверяют эти данные на предмет соответствия заданным в коде условиям, и в случае наличия такого соответствия автоматически запускается выполнение смарт-контракта.

60. В данном случае ключевыми являются слова «безопасные и достоверные данные». Блокчейны не могут и не должны хранить большие объемы данных, поэтому информация должна поступать в блокчейн через приложение-оракул. Из-за этого оракул (как и пользовательский интерфейс) является слабым звеном в обеспечении безопасности и целостности блокчейна. Кроме того, в случае оракулов действует известный принцип, согласно которому использование некорректных данных приводит к получению некорректных результатов (хотя в случае блокчейна использование некорректных данных может привести к необратимому нарушению работы блокчейна). Поэтому в целях обеспечения качества и целостности данных и связанных с ними процессов крайне важно, чтобы в приложениях на базе блокчейн была тщательно продумана процедура сбора информации для оракулов, равно как и их интерфейс для взаимодействия с блокчейном.

3. Интернет вещей и технология блокчейн

61. Термин «Интернет вещей» (IoT) обозначает технологию оборудования физических объектов датчиками и небольшими вычислительными устройствами или интегральными схемами, которые обмениваются данными через Интернет. Обмен данными может осуществляться между объектами, с более крупными компьютерами и вычислительными системами и даже с людьми; например, современные системы обеспечения безопасности жилых помещений в случае регистрации движения уведомляют об этом домовладельца и позволяют подключиться к видеокамере, установленной внутри жилого помещения.

62. IoT-устройства могут собирать самые разнообразные данные. К числу примеров данных, касающихся торговли и перевозок, которыми могут обмениваться IoT-устройства, относятся: информация о местоположении и перемещении грузовика или контейнера, полученная с помощью системы GPS, информация об открытии и закрытии дверей контейнера, данные о температуре внутри контейнера, информация о внешнем воздействии, которому подвергаются контейнеры/поддоны/товары, а также, в случае весьма дорогостоящих товаров, например некоторых лекарственных препаратов или предметов роскоши, информация для отслеживания и идентификации отдельных упаковок или изделий.

63. IoT-устройства могут быть полезны для сбора данных, которые анализируются другими системами, передающими затем результаты этого анализа в блокчейн (т. е. системами, выступающими в роли оракулов блокчейна), или же IoT-устройства могут сами выступать в роли оракула, предоставляя данные непосредственно блокчейну. Вместе с тем IoT-устройства непосредственно в качестве оракулов, как правило, не используются по соображениям безопасности, а также потому, что системы, подключенные к десяткам тысяч IoT-устройств, могут испытывать перегрузку из-за больших объемов данных. Кроме того, в сетях, где за совершение каждой записи необходимо платить небольшую сумму денег, постоянная регистрация значений данных в блокчейн может быть затратной. Поэтому зачастую IoT-данные либо фильтруются, с тем чтобы обмен осуществлялся только в случае данных, значения которых выходят за пределы определенных диапазонов, либо передаются на заключительном этапе процесса в виде полного набора значений.

64. Классическим примером использования блокчейном IoT-данных является страхование товаров, чувствительных к изменению температуры (например, фруктов, которые во время транспортировки должны храниться при температуре от 4 до 15 °C). Во время транспортировки встроенное в контейнер IoT-устройство регистрирует данные, свидетельствующие о том, что в течение двух суток фрукты хранились при температуре 0 °C. Эта информация передается смарт-контракту, который уведомляет страховую компанию о том, что экспортеру причитается компенсация за ущерб, нанесенный его товару из-за слишком низкой температуры, и автоматически производит выплату без какого-либо дополнительного вмешательства со стороны импортера, экспортера или транспортной компании. Таким образом удастся значительно снизить затраты страховых компаний на обработку страховых требований, так как им не нужно сверять информацию, представленную грузоотправителем/экспортером, со страховым полисом, оценивать обоснованность

страхового требования (доказательства предоставляются в виде IoT-данных) и оформлять требование об осуществлении выплаты. При этом издержки для грузоотправителей/экспортеров также сокращаются, так как им больше не нужно собирать дополнительные документы, подтверждающие наступление страхового случая, а страховые суммы выплачиваются им быстрее.

Е. В каких случаях использование блокчейнов целесообразно, а в каких нет

65. Решение о внедрении технологии блокчейн, будь то в государственном или частном секторе, должно приниматься как деловое решение с учетом того, может ли данная технология помочь в одной из следующих задач:

- предоставление новых и улучшенных услуг;
- ускорение процессов и/или проектов по внедрению;
- повышение экономической эффективности процессов и/или проектов по внедрению.

66. Определившись с выбором бизнес-процесса, в отношении которого может быть использован блокчейн, на следующем этапе анализа может быть целесообразно использовать схему принятия решений, представленную на диаграмме ниже.



Диаграмма 1: В каких случаях целесообразно использовать технологию блокчейн⁷

67. Если в ответах на вопросы, представленные на диаграмме 1, ответ «Нет» встречается только один раз, то использование блокчейна все еще может быть оправданным (например, если основным активом является защищенный от взлома реестр или если те, кто имеет разрешение на ознакомление с записями, не доверяют тем, кто имеет разрешение на внесение записей). Кроме того, в некоторых случаях решение на основе баз данных будет вполне приемлемым, однако решение на базе блокчейна может быть реализовано быстрее и/или дешевле, поэтому фактор времени и затрат также важно учитывать.

68. Важно помнить, что использование блокчейна подразумевает применение определенного типа удостоверения подлинности и что не для всех транзакций

⁷ Mr. Anil John, Technical Director, U.S. Department of Homeland Security, Science and Technology, «Beyond Blockchain Basics», at the Annual Computer Security Applications Conference, 5 December 2018, https://www.acsac.org/2018/openconf/modules/request.php?module=oc_program&action=page.php&id=42 (accessed 24 December 2018).

требуется столь высокий уровень надежности. В Типовом законе об электронной торговле, принятом ЮНСИТРАЛ в 1996 году, особо подчеркивается, что способ, выбранный для удостоверения подлинности, должен быть «настолько надежным, насколько это соответствует цели, для которой электронное сообщение было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности»⁸.

69. Следует также принимать во внимание связанные с технологией блокчейн невидимые вычислительные затраты. Даже в том случае, когда такая технология предлагается на бесплатной основе, на последующих этапах производственно-сбытовой цепочки все равно возникают издержки, которые, в зависимости от целого ряда факторов, могут привести к увеличению окончательной стоимости для потребителя, поэтому необходимо проводить тщательный анализ выгод и издержек. Важно также обеспечить условия, при которых использование технологии блокчейн не будет приводить к созданию препятствий для микро-, малых и средних предприятий, а также для стран с развивающейся/переходной экономикой.

70. Хотя многие организации пришли к выводу о том, что в их отрасли имеется потенциал для повышения эффективности процессов за счет использования технологии блокчейн, в данный момент они не приступают к немедленному внедрению этой технологии, а скорее проводят анализ возможности ее внедрения. В ситуации, когда не существует готового блокчейн-приложения, которое организация могла бы сразу же начать использовать, такой подход, вероятно, является наилучшим, учитывая новизну технологии блокчейн и то, что в приложении ко многим процессам она остается непроверенной. Кроме того, иногда организации желают организовать внутреннее тестирование подходов на базе блокчейн, чтобы наработать опыт и выявить любые необходимые изменения, затрагивающие их внутренние процедуры или структуру, прежде чем принять решение о присоединении к одной из все более многочисленных, охватывающих целые отрасли блокчейн-платформ, которые создаются в настоящее время и разработчики которых уже предлагают готовые решения или обещают сделать это в ближайшем будущем.

71. Метод анализа возможности внедрения, как правило, заключается в осуществлении проекта, нацеленного на проверку состоятельности концепции (ПСК), в случае успеха которого рассматриваются возможности осуществления более крупного экспериментального проекта, а затем и внедрения приложения в масштабах всей организации.

72. Даже в случае неудачи реализация проекта ПСК может помочь компании лучше понять назначение технологии и опасности, связанные с ее внедрением, что в будущем поможет компании лучше оценить возможности ее использования в других областях.

73. Если после проведения вышеуказанного анализа организация принимает решение о продолжении работы по проекту ПСК и, в конечном счете, о внедрении технологии, то ее следующим шагом должен стать выбор блокчейна для использования. Все блокчейны имеют особенности и различаются между собой по используемым способам достижения консенсуса, применяемым криптографическим алгоритмам, размерам сети, а также по тому, являются ли они закрытыми или контролируруемыми блокчейнами (см. описания выше). Следует обратить внимание на некоторые ключевые характеристики блокчейнов:

- **уязвимость:** устойчивость ко взломам и другим системным сбоям;
- **надежность:** эффективность устранения таких проблем, как недостатки кода или взломы;
- **затраты:** стоимость транзакций, которая иногда называется «топливом»;

⁸ См. также Рекомендацию ЕЭК ООН 2014 года № 14 «Удостоверение подлинности внешнеторговых документов»: https://www.unece.org/fileadmin/DAM/cefact/recommendations/rec14/ECE_TRADE_C_CEFAC2014_6R.pdf.

- **скорость и масштабируемость:** применимость в случае больших объемов транзакций;
- **уровень защиты конфиденциальности:** полное отсутствие анонимности/использование псевдонимов/полная анонимность, а также соблюдение положений законодательства, направленных на защиту неприкосновенности частной жизни.

74. Для проведения оценки этих характеристик важно прежде всего определить конкретные потребности и проблемы организации в вышеуказанных областях. После этого с учетом выявленных потребностей организация может провести оценку имеющихся вариантов использования технологии блокчейн. Например, если та или иная организация занимается отслеживанием поставок огурцов, то ее потребности в обеспечении защиты от атак хакеров (в снижении уязвимости), вероятно, будут меньше, чем если бы она занималась отслеживанием партий алмазов; с другой стороны, объемы отслеживаемых партий огурцов, скорее всего, значительно превышают объемы отслеживаемых партий алмазов, вследствие чего важное значение приобретает масштабируемость, а из-за низкой стоимости огурцов возникает острая потребность в сокращении затрат.

75. Наконец, при выполнении этого последнего шага убедитесь в том, что вы используете данные, полученные в течение последних 12 месяцев. Технологии блокчейн – быстро развивающаяся область, в которой поиском решений конкретных проблем, возникающих в различных моделях блокчейна, занимается множество специалистов. Поэтому то, что было актуально 2 года или даже 18 месяцев назад, сегодня может не соответствовать действительности. Весьма полезными могут оказаться консультации с программистами, имеющими богатый опыт в области внедрения технологии блокчейн, так как зачастую решения, позволяющие обойти те или иные проблемы, уже были найдены, особенно в случае открытых блокчейнов, которыми занимается большее число экспертов.

Приложение

<i>Сектор</i>	<i>Заполняется только в том случае, если информации, представленной в названии главы, недостаточно</i>
Краткое описание	1–2 предложения или не более 240 знаков
Предлагающая/осуществляющая/тестирующая организация	Если не применимо или если сведения отсутствуют, просьба написать «Н.П.»
Контактное лицо для получения дополнительной информации	Имя и адрес электронной почты (минимальная информация), также можно указать: <ul style="list-style-type: none"> • номер(а) телефона(нов) и/или • почтовый адрес и/или • веб-сайт
Подробное описание	Не более 1 200 знаков
Потенциальные преимущества для предприятия от использования технологии блокчейн	Следует указывать только преимущества, извлекаемые благодаря особым характеристикам блокчейна, т. е. преимущества, которые не могут быть получены с помощью других технологий
Особые вопросы, вызывающие опасения (правового, технического характера и т. д.)	Могут включать в себя аспекты, варьирующие от потребности в обеспечении минимального времени реагирования до необходимости правового признания или соблюдения требования относительно минимального количества членов консорциума или сетевых узлов
Используемый/предлагаемый блокчейн	Bitcoin, Bitcoin Cash, Ethereum, Consortium, Private и т. п.
Тип алгоритма консенсуса (является ли блокчейн закрытым или контролируемым/управляемым консорциумом)	Если не применимо или если сведения отсутствуют, просьба написать «Н.П.»
Мотивация, а также преимущества и недостатки, которые учитываются при выборе блокчейна	Если не применимо или если сведения отсутствуют, просьба написать «Н.П.»
Любое специальное компьютерное и прочее используемое оборудование (IoT, QR-коды и т. д.)	Если не применимо или если сведения отсутствуют, просьба написать «Н.П.»
Любое используемое/предлагаемое программное обеспечение с открытым исходным кодом	Если не применимо или если сведения отсутствуют, просьба написать «Н.П.»
Ссылки на сопутствующую информацию, включая технические «белые книги»	Если не применимо или если сведения отсутствуют, просьба написать «Н.П.»