Павел С. Ложников, Алексей Е. Сулавко, Самал С. Жумажанова
ФГБОУ ВО «Омский государственный технический университет»,
пр-т Мира, 11, г. Омск, 644050, Россия
e-mail: lozhnikov@mail.ru, http://orcid.org/0000-0001-7878-1976
e-mail: sulavich@mail.ru, http://orcid.org/0000-0002-9029-8028
e-mail: samal_shumashanova@mail.ru, http://orcid.org/0000-0002-6785-5201

О ВОЗМОЖНОСТИ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ РАСПРЕДЕЛЕННОГО РЕЕСТРА В СИСТЕМЫ СМЕШАННОГО ДОКУМЕНТООБОРОТА*

DOI: http://dx.doi.org/10.26583/bit.2019.1.02

Аннотация. В работе приведено исследование возможности применения технологий распределенного реестра в управлении различными бизнес-процессами, опирающимися на системы электронного документооборота. В сфере финансов и торговли разновидность технологии распределенного реестра – блокчейн – уже представлена как реальная альтернатива существующей инфраструктуре, однако опыта создания и внедрения таких решений в системы электронного документооборота на данный момент недостаточно. Предложенная ранее авторами модель гибридного документооборота имеет ряд преимуществ над привычной схемой информационного обмена, так как сочетает равную защиту документа в аналоговой и цифровой форме с применением криптографических и биометрических методов. Схема гибридного документооборота на базе технологий распределенного реестра обеспечивает децентрализованное хранение информации, фиксированный объем хранимых и передаваемых пользователями блоков данных, выработку криптографических ключей с применением биометрических образов допущенных к работе пользователей и идентификацию субъектов, производивших различные действия с документом независимо от типа его носителя. В работе рассмотрены возможные проблемы информационного взаимодействия, с которыми общество может столкнуться при разработке и внедрении схемы гибридного документооборота.

Ключевые слова: системы электронного документооборота, гибридный документ, системы распределенного реестра, блокчейн-технологии, биометрия, электронная цифровая подпись.

Для цитирования: ЛОЖНИКОВ, Павел С.; СУЛАВКО, Алексей Е.; ЖУМАЖАНОВА, Самал С. О ВОЗМОЖНОСТИ ВНЕДРЕНИИ ТЕХНОЛОГИЙ РАСПРЕДЕЛЕННОГО РЕЕСТРА В СИСТЕМЫ СМЕШАННОГО ДОКУМЕНТООБОРОТА. Безопасность информационных технологий, [S.l.], p. 15-24, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1176>. Дата доступа: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.02.

Благодарности. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-07-01204.

Pavel S. Lozhnikov, Alexey E. Sulavko, Samal S. Zhumazhanova
Omsk State Technical University,
Mira ave., 11, Omsk, 644050, Russian Federation
e-mail: lozhnikov@mail.ru, http://orcid.org/0000-0001-7878-1976
e-mail: sulavich@mail.ru, http://orcid.org/0000-0002-9029-8028
e-mail: samal_shumashanova@mail.ru, http://orcid.org/0000-0002-6785-5201

About the possibility of embedding the distributed ledger technologies into the systems of mixed workflow*

DOI: http://dx.doi.org/10.26583/bit.2019.1.02

Abstract. The paper presents a study on the possibility of using distributed ledger technologies in managing various business processes based on electronic document management systems. In the finance and trade sphere, the type of distributed ledger technology, blockchain, is already presented as a real alternative to the existing infrastructure, however, the experience of developing and implementing such solutions in electronic document management systems is currently insufficient. The model of hybrid workflow proposed earlier by the authors of the article has a number of advantages over usual scheme of information exchange, and combines equal document protection in paper and digital form using cryptographic and biometric methods. The described distributed ledger-based hybrid workflow scheme also provides decentralized information storage, a fixed size of data blocks stored and transmitted by

users, generation of cryptographic keys using biometric images of authorized users, and identification of subjects that performed various actions on document regardless of its type format. The authors also considered possible problems that might be encountered in the development and implementation of such an information interaction scheme.

Keywords: electronic document management systems, hybrid document, distributed ledger technology, blockchain, biometrics, electronic signature.

For citation: LOZHNIKOV, Pavel S; SULAVKO, Alexey E.; ZHUMAZHANOVA, Samal S. About the possibility of embedding the distributed ledger technologies into the systems of mixed workflow. IT Security (Russia), [S.l.], p. 15-24, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1176>. Date accessed: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.02.

***Acknowledgement.** The reported study was funded by RFBR according to the research project № 16-07-01204.

Введение

Выполнение бизнес-процесса часто реализуется путем последовательного манипулирования документом, передаваемым от одного агента/сотрудника к другому. Документ, как часть бизнес-процесса, может иметь ограничения на способ его модификации и на круг лиц, имеющих разрешение на подобные модификации. Эти ограничения являются неотъемлемой частью жизненного цикла документа. В терминах ограничений, применяемых к документу, последовательность манипуляций считается действительной до тех пор, пока каждый документ следует его собственному жизненному циклу на всех этапах рабочего процесса [1].

Существуют два основных подхода к обеспечению корректности жизненного цикла документа. Первый заключается в том, что все участники процесса, вовлеченные в манипуляции с документом, доверяют друг другу и предполагают, что они выполняют только корректные действия с документом. В противном случае все участники бизнес-взаимодействия могут доверять третьей стороне; эта сторона несет ответственность за соблюдение корректности жизненного цикла документа и должна предотвратить несанкционированные изменения. Важно отметить, что оба сценария требуют определенной формы внешнего доверия, которая является отправной точкой для атак. В первом случае один злонамеренный пользователь может помешать корректному исполнению жизненного цикла и аннулировать любые доверительные гарантии, которые могут иметь другие партнеры по отношению к нему. Во втором сценарии зависимость от третьей стороны открывает путь к классическим атакам, таким как «человек посередине».

Рост объемов цифровых данных, имеющих определенную ценность для их владельцев, побуждает к разработке более эффективных методов хранения и обеспечения целостности и доступности такой информации. Технология распределенного хранения данных, представленная в виде разновидностей системы распределенных реестров (далее – СРР), с этой точки зрения позволяет получить ряд преимуществ ее пользователям. СРР является базой данных различных активов, резервные копии которых хранятся на всех узлах сети, доступ к этой базе имеют все участники сети из любого уголка планеты. Такое хранение позволяет заметить любые изменения данных, что уже через несколько секунд будет отражено в остальных копиях. Частным случаем СРР является блокчейн-технологии – одноранговые системы для объединения постоянно растущих списков упорядоченных записей, называемых блоками, в связанную цепочку. Каждый блок цепи содержит метку времени и ссылку на предыдущий блок. При случайном/умышленном изменении одного из блоков, результирующий хэш-код блоков будет совершенно другим. Каждый участник «цепочки» хранит у себя точную копию исходного реестра, что позволяет заметить малейшие изменения во всей цепочке. Изменить данные в конкретном блоке не представляется возможным. Защита от несанкционированного доступа к блокам может быть реализована шифровальными и криптографическими средствами, которые обеспечивают доступ пользователю только к тем записям, которые он вносил самостоятельно. Усилия, требуемые для взлома децентрализованной базы данных,

являются титаническими и в большинстве случаев даже не стоят потраченного на это времени [2].

В рамках блокчейн-технологий предлагается дополнительная концепция «умных контрактов» [3], в которых бизнес-процессы подчиняются правилам реагирования на конкретные условия. Умный контракт (англ. Smart contract) представляет собой компьютерный код, работающий поверх цепи блоков, содержащей набор правил, в соответствии с которыми стороны этого контракта соглашаются взаимодействовать друг с другом. Когда сторонами соблюдены предварительно определенные правила, то соглашение автоматически применяется. Код интеллектуального контракта облегчает, проверяет и обеспечивает согласование и выполнение операций. Этот способ проверки корректности жизненного цикла документа в отличие от множества существующих вариантов состоит в том, что сам документ предназначен для переноса фрагментов своей истории, защищенных от несанкционированного доступа с использованием хэширования и шифрования. Такой документ принято называть «интеллектуальным». Любой руководитель, а также иной участник процесса может в любой момент проверить, соответствует ли история документа данному жизненному циклу.

1. Социально-правовые проблемы, связанные с внедрением СРР на базе блокчейн-технологий в системы документооборота

В настоящее время споры вокруг СРР на базе блокчейн-технологий сосредоточены в основном на технических аспектах внедрения «умных» контрактов и их реализации в рамках конкретной технологической основы. Большое внимание уделяется эффективности и оптимизации ее использования с целью обеспечения необходимого уровня безопасности, который в то же время превосходит традиционное законодательство в сфере договорных отношений и снижает другие транзакционные издержки, связанные с контрактом. Различные системы на базе блокчейн-технологий все еще находятся на стадии тестирования, и в их реализации имеется ряд технических проблем, которые необходимо решить, например, задержки при выполнении транзакций, пропускная способность (число выполняемых транзакций в единицу времени), масштабируемость, размер хранимых данных, защита от разного рода атак и т.д. Помимо указанных проблем применение СРР на базе блокчейн-технологий не может не вызывать вопросов социально-политического, экономического характера, внося существенные корректировки в каждую из указанных областей.

Ряд специалистов считает, что о правовом регулировании блокчейн-технологий говорить пока рано. Это станет возможным, когда появятся предпосылки к их массовому использованию. Отметим, что, когда впервые появился Интернет, изначально правительства не уделяли этому должного внимания. Но поскольку эта технология стала фундаментальной силой, влияющей на торговлю, СМИ, коммуникации и т.д., правительства многих стран начали устанавливать ограничения и правила по ее использованию. То же самое можно предположить и для блокчейн-технологии, которая все еще находится на ранней стадии развития, по сравнению с Интернетом начала 90-х. Некоторые правительства изучают блокчейн-технологию и ее применение [4] с целью повышения эффективности предоставления государственных услуг. Однако не все осознают целесообразность вложений, так как не уверены в широком диапазоне экономических и социальных мероприятий, в которых потенциально может иметь место нерегулируемая и децентрализованная система на базе блокчейн-технологии. Например, наблюдается отказ регулирующих органов США от фонда обмена Bitcoin. В частности, технология одноранговой сети, скорее всего, не будет приветствоваться правительствами, которые хотят сохранить контроль над финансовым и информационным секторами государства.

В то же время важно не избегать вопроса внедрения и правового регулирования блокчейн-технологии особенно когда дело доходит до возможных видов использования криптовалютных транзакций для хищения денежных средств, уклонения от налогов и

осуществления незаконной деятельности на «черном» рынке – риск остается реальным и может оказать существенное негативное воздействие на общество. Уже сейчас эксперты выделяют несколько аспектов, с которыми столкнется общество в ближайшем будущем относительно использовании блокчейн-технологии:

• «цифровые» доказательства в судебных спорах;
• оборот криптовалют при расчетах между юридическими лицами;
• автоматизацию и децентрализацию юридических процессов.

Внедрение системы электронного документооборота на базе блокчейн-технологии предполагает ввод документа в цифровой форме, и это является существенной проблемой для смешанного документооборота. Способ оцифровки документов и извлечения информации, которая позволит определить целостность и аутентичность документа, разработан ранее авторами настоящей статьи [5]. Был предложен формат гибридного документа, который помимо информационного контента как в аналоговой, так и в цифровой форме содержит в себе информацию о создателе документа, электронную цифровую подпись (ЭЦП), ссылку на облачный сервер для проверки хэш-кода документа. Данная информация накладывается на документ в виде считываемых QR-кодов вместе с секретной информацией, сокрытой методами стеганографии. Секретная информация содержит те же данные, что и QR-код, и это позволяет авторизованному пользователю определить факт несанкционированных изменений. Такая модель документооборота способствует обеспечению равной защиты документа как в цифровой, так и в аналоговой форме.

Однако для стандартизации, с точки зрения технологии на базе блокчейн-технологий, она еще не достигла такого уровня, который позволил бы обеспечить ее эффективное внедрение, так как не касается всех аспектов, необходимых для построения целостной системы.

2. Сложности контроля доступа к документам на бумажном носителе

Ограничения по отношению к документу делятся на три группы [6]:

1) *ограничения контроля на доступ* представляют собой запрет или разрешение на конкретные действия с определенными фрагментами документа определенному кругу лиц. Приведем примеры таких ограничений из сферы медицинского информационного обмена:

– ограничения на просмотр фрагмента: например, врач не может прочитать номер страховки пациента, в то время как страховая компания не может видеть медицинскую информацию;

– ограничения на модификацию фрагмента: например, фармацевт может просматривать поле с рецептом от врача, но не может его изменить;

2) *ограничения целостности* – это обеспечение того, что данные, к которым имеется легитимный доступ, не были изменены или повреждены с момента последнего корректно совершенного действия с этим документом. Например, партнерам из одной организации должен быть передан именно последний подписанный руководителем другой организации вариант договора;

3) *ограничения жизненного цикла* – это ограничения на порядок, в котором могут быть выполнены корректные действия. Если действие совершается «вне порядка», документ все еще будет читаемым, но ознакомление с его историей покажет эту несогласованность. Например, договор может быть подписан главным бухгалтером организации только после подписания его начальником юридического отдела. Если вновь обратиться к медицинской сфере, то примером ограничения жизненного цикла здесь является требование о том, чтобы рецепт был одобрен страховой компанией до того, как он может быть заполнен фармацевтом.

На сегодняшний день часть бизнес-процессов являются автоматизированными и большинство действий со значимыми документами происходят в системах электронного документооборота (ЭДО). Развитие информационных технологий позволяет

интегрировать в привычный для нас формат электронных документов современные технические решения, которые обеспечивают соблюдение упомянутых ограничений, например, усиленная электронная цифровая подпись (ЭЦП) – реквизит, позволяющий проверить отсутствие искажения информации, принадлежность подписи владельцу сертификата ключа подписи, а также подтвердить факт подписания электронного документа.

Однако, как показывает практика, полностью «безбумажного» документооборота в ближайшее время ожидать не придется, так как нормативно-правовыми актами Российской Федерации предусмотрено наличие определенного рода документов только в бумажной форме, заверенных соответствующими реквизитами; во-вторых, большинству руководителей и сотрудников просто удобен такой способ представления документов для ознакомления и утверждения. Поэтому на сегодняшний день наблюдается развитие смешанного документооборота, в котором в процессе своего жизненного цикла документ может прибывать как в электронной, так и в бумажной форме.

Как в электронной, так и в бумажной форме документ имеет ряд уязвимостей и подвержен атакам со стороны внутреннего и внешнего нарушителя, целью которых является доступ к документу в обход описанных ограничений. Например, рукописная (физическая) подпись, нанесенная на бумажный документ, может быть подделана так, что принимающая сторона не сможет отличить ее от оригинала; электронный документ, визированный ЭЦП, может быть подписан не юридическим владельцем ЭЦП, а, например, сотрудником, которому доверили подписание документа или иным лицом, получившим носитель ЭЦП.

Проблемы отчуждения ЭЦП (секретного ключа) от его владельца, их ненадлежащего хранения, подделки третьими лицами (рукописной подписи) на данный момент находятся на стадии решения. Авторы настоящей работы и остальные участники научного коллектива разработали концепцию «гибридного документооборота» [5], отличительной особенностью которой является в том числе использование биометрических образов пользователей при формировании ЭЦП для обеспечения равной защиты документов в любой форме их представления. Биометрические образы в данном случае представляют собой особенности воспроизведения подписи, клавиатурного почерка и параметры лица (рис. 1).

Рис. 1. Структурная схема системы защищенного гибридного документооборота
(Fig. 1. The block diagram of a system protected by hybrid workflow)

Предложенная концепция изменяет привычный маршрут документа в смешанном документообороте (рис. 2).

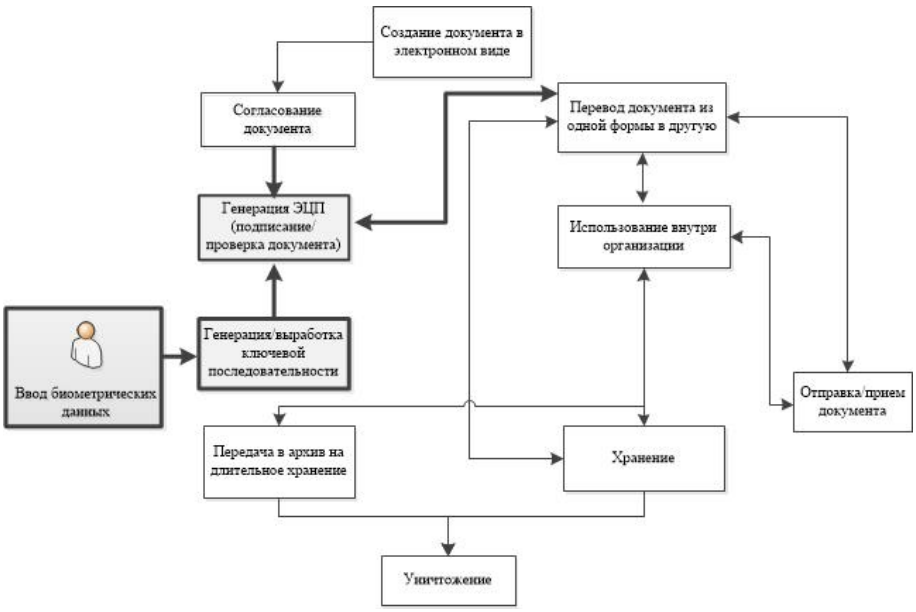

Рис. 2. Модифицированная схема маршрута документа в смешанном документообороте, общий случай. Жирными линиями обозначены введенные модификации.
(Fig. 2. The modified route scheme document, a mixed document, the General case. Bold lines indicate the modifications introduced.)

Несмотря на преимущества данного подхода по сравнению с существующими методами защиты, возможность обеспечения аутентичности документа в любой форме, проверка такого документа требует обращения принимающей стороны (начальник другого отдела в организации, руководитель другой организации) к облачному хранилищу/серверу по ссылке, которой снабжен гибридный документ. Использование централизованного хранилища подразумевает, что файлы владельца документа, а также других пользователей, метаданные хранятся в конкретном месте, что, с одной стороны, удобно для всех участников документооборота, однако увеличивает вероятность потери данных, их удаления или изменения третьими лицами.

Хранение ключевой информации и биометрического эталона субъекта должно быть безопасным [7]. Для этого разрабатываются преобразователи «биометрия-код» (ПБК), способные преобразовывать вектор нечетких, неоднозначных биометрических параметров «Свой» в четкий однозначный код ключа (пароля) [8]. Найден способ, позволяющий пользователям безопасно хранить свои персональные биометрические и криптографические данные в нейросетевых контейнерах. В работе [9] для этой цели предлагается построить гибридную нейронную сеть, состоящую из различных функционалов (мер близости), например, взвешенных сумм классических персептронов, квадратичных форм и их разновидностей, многомерных корреляционных, гиперболических и разностных функционалов Байеса. Таким образом, удается получить существенный выигрыш в показателях интегральной ошибки распознавания субъектов. Нейросетевой ПБК настроен на выработку ключа ЭЦП, который генерируется заранее заданным криптографическим алгоритмом после предъявления пользователем своего биометрического образа. Биометрический эталон и данные для генерации ключа хранятся в нейросетевом ПБК в виде таблицы нейросетевых функционалов таким образом, что извлечь одну составляющую вычислительно сложно без знания другой. Внедрение нейросетевых ПБК снимает вопрос о месте хранения секретного (закрытого) ключа пользователя. Обученный ПБК можно разместить на рабочем месте, сервере и т.д.

Метаданные – это сопроводительная информация, которая подтверждает действительность основного контента – документа. В группу таких сведений могут входить данные об учетной записи (идентификатор), открывшей документ, внесшей изменения и т.д., точное время подписания документа, права доступа, иная информация. Для таких данных прежде всего необходимо обеспечить их неизменность. При одном

успешном доступе неавторизованного (незарегистрированного) пользователя к централизованному хранилищу, где размещены метаданные, сложно будет доказать их подмену. На сегодняшний день этот вопрос можно решить с помощью внедрения СРР.

3. Интеграция СРР в систему документооборота

Потенциал СРР на основе блокчейн-технологий успешно протестирован для обеспечения совместной работы в открытых средах в различных областях: от торговли алмазами до расчетов по ценным бумагам [10], при создание новых финансовых инструментов, таких как Bitcoin. Данная технология, скорее всего, найдет свое применение в организациях не только для решения финансовых вопросов.

Основные свойства блокчейн-технологий [11]:

- децентрализованность;
- публичность;
- консенсус (взаимное согласие) участников;
- отсутствие посредников (внешние органы, центры сертификации и т.д.).

Данная технология также усиливает существующие свойства, связанные с основными элементами проверки документов:

- целостность: обеспечение того, чтобы копия документа имела то же содержание, что и оригинал;
- аутентичность: подтверждение авторства документа;
- невозможность отказа: отсутствие возможности отрицать, что субъект просмотрел, создал или изменил документ, до тех пор, пока каждая итерация сохраняется в цепочке блоков. Первое может соблюдаться в том случае, если в системе предусмотрена процедура подписания документа секретным ключом пользователя только после его ознакомления с содержимым.

Поскольку механизм проверки документа «живет» в цепочке, пользователям сложно манипулировать документом без последующего обнаружения этого факта участниками цепочки, т.е. имеется возможность проследить историю документа в ходе его жизненного цикла.

В предложенной схеме (рис. 3) список узлов для хранения блоков цепи ограничен только участниками документооборота, на практике же может быть расширен лицами вне этого взаимодействия. Варианты проверки ограничений, накладываемых на документ, не отличаются от типичной схемы, применяемой в системах на базе блокчейн-технологий. Однако здесь также применяется концепция гибридного документооборота, которая подразумевает выработку закрытого ключа с помощью биометрических данных пользователя при каждой попытке подписания документа [12] с помощью ПБК. Открытые ключи пользователей генерируются вместе с закрытыми ключами и хранятся на рабочих местах пользователей и/или на сервере. Каждый участник хранит у себя список адресов остальных пользователей, каждый из которых он сравнивает с информацией внутри вновь поступившего блока. В реестре также должна храниться информация о некорректных изменениях в документе, например, нарушение порядка доступа к документу и идентификатор пользователя, внесшего эти изменения. Также стоит учесть, что отдельному участнику документооборота может быть доступна работа только с частью документа, однако это ни в коем случае не лишает его права на проверку целостности, аутентичности и истории документа (для этого применяется проверка хэш-кода).

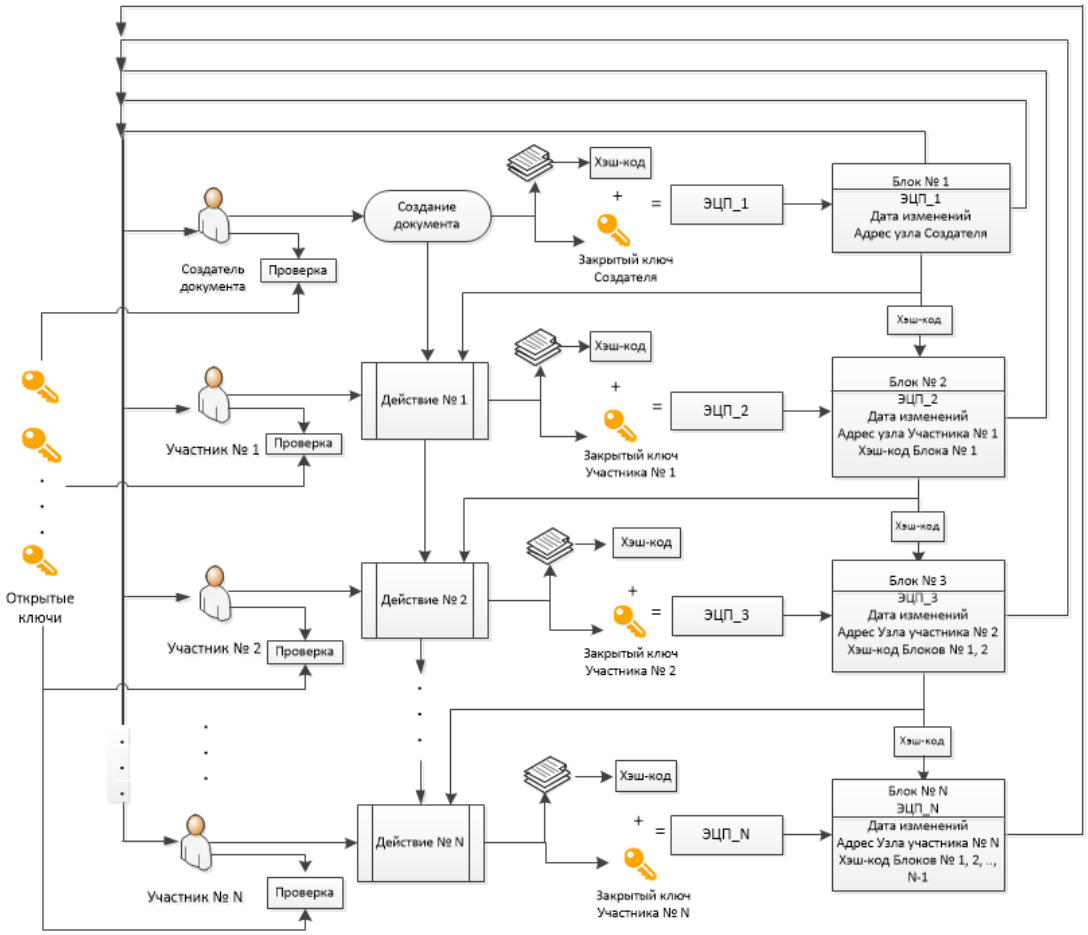

Рис. 3. Схема электронного документооборота с использованием блокчейн-технологий (Fig. 3. The scheme of electronic document flow using blockchain)

По мере того как все больше предприятий продвигаются по пути внедрения ЭДО, одной из немаловажных проблем является возможность совместной работы над контентом. Обычно для этого требуется отправка одного документа адресату и обратно, причем только один человек редактирует его за раз (остальные блокируются с целью сохранения контроля версий). Блокчейн-технологии в целом позволят устранить вопрос о месте хранения «главного» документа. В отличие от Google Docs и подобных решений при внедрении блокчейн-технологии каждый узел сети будет хранить копию цепи блоков. Документ может находиться в распределенной, децентрализованной сети, и любые изменения (изменения оригинала) могут быть немедленно идентифицированы и проверены с помощью открытого ключа – обеспечивается сохранение целостности посредством прозрачности изменений. Однако такой способ хранения данных вызывает проблему роста информационной емкости блоков данных, которая в недалеком будущем может стать актуальной. В системе Bitcoin такая ситуация может возникнуть из-за указания максимального размера блока данных, а также роста транзакций, которые необходимо хранить в блоке ограниченного объема. Ряд источников утверждают, что на данный момент объем хранимых пользователями данных в системе Bitcoin уже превышает 200 Гб и начиная с 2010 года растет экспоненциально [13]. Пока основным решением такой проблемы является увеличение исходного размера блока в два раза. Если учитывать, что число участников информационного обмена в рамках ЭДО может быть абсолютно любым, как и число вносимых ими изменений в документ, то остается вариант с централизованным хранением документа, изменения в которые вносятся в заранее оговоренной участниками последовательности и соблюдаются системой контроля версий.

Чтобы решить вопрос роста объема данных в рамках системы гибридного документооборота, необходимо понять, какие данные обязательны для хранения в блоке цепи, чтобы по ним однозначно идентифицировать пользователя и проверить целостность

данных. Стоит напомнить, что для ключевого элемента документооборота – документа – записи в блоки цепи позволяют подтвердить его целостность и аутентичность. Цифровой отпечаток документа и иной информации в виде истории документа (хэш-код), ЭЦП и метаданные имеют фиксированный размер для любого объема данных (табл. 1). История всех предыдущих изменений хранится в одном хэш-коде, таким образом, все блоки цепи имеют одинаковый размер, кроме самого первого, который имеет наименьший объем. С учетом особенностей документооборота для того, чтобы избежать переполнения данных на рабочих местах пользователей, при взаимном согласии участников им необходимо хранить только последние несколько блоков цепи либо ограничить «время жизни» каждого блока. С этой целью необходимо внести ограничения на временной промежуток, который необходим для внесения изменений в документ для каждого пользователя, число манипуляций с документом в сутки (неделю) для каждого пользователя, при этом важно обеспечить подписание каждого документа (или блока) всеми участниками после ознакомления с ним, чтобы хранить в цепочке только последние подписанные всеми пользователями блоки. Вся цепь, содержащая информацию обо всех операциях с документом, может быть занесена в архив или храниться вместе с документом на сервере.

Таблица 1. Блок данных в предложенной схеме документооборота
(Table 1. A block of data in the proposed scheme of document workflow)

Блок для отправки на узлы цепочки				
• ЭЦП=Хэш-код документа + закрытый ключ	• Дата изменений	• Хэш-код адреса узла Пользователя	• Права доступа	• Хэш-код хэш-кодов предыдущих блоков

Заключение

В работе продемонстрирована возможность внедрения системы распределенных реестров, в частности блокчейн-технологий, в существующую модель электронного (гибридного) документооборота. История транзакций с защитой от несанкционированного доступа с применением нейросетевых преобразователей «биометрия-код» может стать существенным улучшением для многих процессов документооборота как внутри организаций, так и между ними. Система распределенных реестров на базе блокчейн-технологий может заполнить недостатки существующих систем, являясь решением, в котором не требуется некий центральный компонент для хранения данных или принятия решения о корректности действий пользователей. Проблема роста объемов хранимых в цепочке блоков данных в предлагаемой схеме решается ограничениями на количество хранимых блоков, время их хранения, а также число операций, которые пользователи могут совершать за определенный период времени.

СПИСОК ЛИТЕРАТУРЫ:

1. Cohn D., Hull R. Business Artifacts: A Data-centric Approach to Modeling Business Operations and Processes // IEEE Data Eng. Bull. 2009. Vol. 32. P. 3 – 9.
2. Fridgen G. et al. Cross-Organizational Workflow Management Using Blockchain Technology - Towards Applicability, Auditability, and Automation. HICSS. 2018.
3. Szabo N. Formalizing and Securing Relationships on Public Networks. First Monday. 1997. Vol. 2, № 9.
4. IBM Building trust in government - United States. 2018. URL: https://www.ibm.com/services/us/gbs/thoughtleadership/blockchain-for-government/ (дата обращения: 18.10.2018).
5. Ложников П.С. Биометрическая защита гибридного документооборота: моногр // Изд-во СО РАН. 2017. 130 с.
6. Hallé S. et al. Decentralized enforcement of document lifecycle constraints // Information Systems. 2018. Vol. 74. P. 117 – 135.
7. Иванов А.И., Фунтиков В.А., Ефимов О.В. Способ защиты персональных данных биометрической идентификации и аутентификации: Патент RU2346397C1. Опубл. 10.02.2009.
8. ГОСТ № 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации, ГОСТ № от 27.12.2006 №52633.0-2006.

9. Lozhnikov P.S., Sulavko A.E. Generation of a biometrically activated digital signature based on hybrid neural network algorithms // IOP Conf. Series: Journal of Physics: Conf. Series. II International scientific conference "Mechanical Science and Technology Update", 27-28 February 2018. Omsk, Russia. Vol. 1050. P. 012047.
10. Walport M. Distributed Ledger Technology: Beyond Blockchain // UK Government Office for Science, Tech. Rep. 19. 2016.
11. Beck R. et al. Blockchain Technology in Business and Information Systems Research // Bus Inf Syst Eng. 2017. Vol. 59, № 6. P. 381 – 384.
12. Еременко А.В., Ложников П.С., Сулавко А.Е. Генерация ключевых последовательностей на основе параметров подсознательных движений // Информационные системы и технологии. 2017. № 1 (99). С. 99 – 109.
13. Bitcoin blockchain size 2010-2018 | Statistic. URL: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ (дата обращения: 06.11.2018).

REFERENCES:

[1] Cohn D., Hull R. Business artifacts: a data-centric approach to modeling business operations and processes. IEEE Data Eng. Bull. 2009. Vol. 32. P. 3 – 9.
[2] Fridgen G. et al. Cross-organizational workflow management using blockchain technology - towards applicability, auditability, and automation. HICSS, 2018.
[3] Szabo N. Formalizing and securing relationships on public networks. First Monday. 1997. Vol. 2, no 9.
[4] IBM Building trust in government - United States. 2018. URL: https://www.ibm.com/services/us/gbs/thoughtleadership/blockchain-for-government/ (accessed: 18.10.2018).
[5] Lozhnikov P.S. *Biometricheskaya zashchita gibridnogo dokumentooborota* [Biometric protection of hybrid workflow: monogr], *Izd-vo SO RAN* [SB RAS Publ.]. 2017. 130 p. (in Russian).
[6] Hallé S. et al. Decentralized enforcement of document lifecycle constraints. Information Systems. 2018. Vol. 74. P. 117 – 135.
[7] Ivanov A.I., Funtikov V.A., Efimov O.V. Sposob zashchity personal'nykh dannykh biometricheskoy identifikatsii i autentifikatsii [*Method of protecting personal biometrical identification and authentification data*]: Patent RU 2346397C1. Published 10.02.2009.
[8] GOST № 52633.0-2006 *Zashchita informatsii. Tekhnika zashchity informatsii. Trebovaniya k sredstvam vysokonadezhnoy biometricheskoy autentifikatsii* [Information Security. Information security techniques. Requirements for highly reliable biometric authentication], GOST № 27.12.2006 no. 52633.0-2006. (in Russian).
[9] Lozhnikov P.S., Sulavko A.E. Generation of a biometrically activated digital signature based on hybrid neural network algorithms. IOP Conf. Series: Journal of Physics: Conf. Series. II International scientific conference "Mechanical Science and Technology Update", 27-28 February 2018. Omsk, Russia. Vol. 1050. P. 012047.
[10] Walport M. Distributed ledger technology: beyond blockchain. UK Government Office for Science, Tech. Rep. 19, 2016.
[11] Beck R. et al. Blockchain Technology in Business and Information Systems Research. Bus Inf Syst Eng. 2017. Vol. 59, no. 6. P. 381 – 384.
[12] Eremenko A.V., Lozhnikov P.S., Sulavko A.E. *Generatsiya klyuchevykh posledovatel'nostey na osnove parametrov podsoznatel'nykh dvizheniy* [Generation of key sequences based on the parameters of the subconscious movements]. *Informatsionnyye sistemy i tekhnologii* [Information Systems And Technologies], 2017, no. 1 (99). P. 99 – 109. (in Russian).
[13] Bitcoin blockchain size 2010-2018 | Statistic. URL: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ (accessed: 06.11.2018).

Поступила в редакцию – 30 октября 2018 г. Окончательный вариант – 31 января 2019 г.
Received – October 30, 2018. The final version – January 31, 2019.