

ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА И ЗАЩИТА ДОКУМЕНТООБОРОТА СУДЕБНОЙ СИСТЕМЫ

Черных А.М. *

Ключевые слова: судебная система, документооборот, блокчейн-сеть, технология блокчейн, электронное делопроизводство, распределенная база данных, система управления базой данных, хеш-функции, алгоритм шифрования сети.

Аннотация.

Цель работы: обоснование возможности создания судебной информационной системы документооборота на блокчейн-платформе, решения задачи обеспечения открытости сервиса для пользователей и поддержания высокой степени защищенности документальных данных всех участников судебного процесса на всем его протяжении.

Метод: информационный и структурный анализ судебных процессов с точки зрения распределенной телекоммуникационной сети, построенной по технологии блокчейн, для решения задач достоверного документооборота на протяжении судебного процесса с учетом обеспечения консенсуса заинтересованных сторон и невозможности внести изменения в используемые в судебном процессе документы без согласия всех участников.

Результаты: обоснована возможность использования блокчейн-технологии при построении информационной системы судопроизводства; рассмотрен переход на электронную регистрацию документов, ведение электронных реестров при взаимодействии участников судебного процесса преимущественно в электронной форме; разработана концептуально-логическая модель документооборота в ходе судебного процесса с использованием распределенного реестра с высокой степенью защищенности информации на длительном временном отрезке, обеспечивающем снижение коррупционной составляющей в системе контроля и учета юридически значимых документов судебного процесса.

DOI: 10.21681/1994-1404-2020-4-20-28

Обеспечение национальных интересов в области свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления возможно путем реализации приоритетных задач по формированию информационного пространства с учетом потребностей населения и общества в получении качественных и достоверных сведений. Развитие информационной и коммуникационной инфраструктуры Российской Федерации, создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне — одна из стратегических задач¹.

¹ Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы». URL: <http://www.pravo.gov.ru>.

* Черных Андрей Михайлович, кандидат технических наук, доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.
E-mail: kafpi@mail.ru

Инфраструктура электронного правительства объединяет размещенные на территории Российской Федерации государственные информационные системы, программно-аппаратные средства и сети связи, обеспечивающие оказание услуг в электронной форме, взаимодействие органов государственной власти Российской Федерации, органов местного самоуправления, граждан и юридических лиц. Таким образом, формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных информационных услуг невозможно без совершенствования нормативного правового регулирования в сфере обеспечения эффективной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение).

Существующие подходы по созданию и ведению информационных систем в судебном делопроизводстве не позволяют гарантировать сохранность как самих документов, так и их содержания на протяжении всего судебного спора. Нередки случаи утраты, изменения, подлога

документов и судебных дел, что ведет к неоправданным судебным решениям или к закрытию судебного производства. В настоящее время существует потребность в обеспечении информационной защищенности документированных данных на протяжении всего судебного процесса, а не только его конечного результата.

В основу формирования единого информационного (цифрового) пространства судебной системы в соответствии с требованиями нормативных документов положены меры по совершенствованию правового регулирования, включающие выработку понятий, необходимых для формирования единой цифровой среды судебной системы [1], где создание алгоритмов удаленного подтверждения личности для совершения юридически значимых действий обеспечивают *конфиденциальность* и *достоверность* [5] данных судебной системы. Введение равного статуса для различных способов идентификации и аутентификации физических и юридических лиц, иных участников системы судебных отношений, правовое признание равных с очными бумажными взаимодействиями цифровых публичных правовых и гражданско-правовых взаимодействий обеспечивает переход к цифровизации не только судебных данных, но и процессуальных отношений. Выработка способов независимой доверенной фиксации и предоставления заинтересованным лицам юридических данных, связанных с электронным, дистанционным взаимодействием и электронными документами третьей доверенной стороны, решает задачу доверия сторонам судебного процесса.

Сегодня, в соответствии с существующими требованиями, обращение в Верховный Суд Российской Федерации и суды различной юрисдикции может быть подано в виде электронного документа или его образа, подписанного усиленной квалифицированной электронной подписью. Судебные акты, за исключением актов, содержащих сведения, составляющие государственную или иную охраняемую законом тайну, если дело рассмотрено в закрытом судебном заседании, выполняются в форме электронного документа, который подписывается судьей (судьями, если судебный акт принят судом коллегиально) также усиленной квалифицированной электронной подписью.

Каждый документ представляется в виде отдельного файла в формате *PDF*, файлы прилагаемых документов могут быть представлены в форматах: *PDF, RTF, DOC, DOCX, XLS, XLSX, ODT* (для документов с текстовым содержанием), *PDF, JPEG (JPG), PNG, TIFF* (для документов с графическим содержанием). Электронный документ должен быть подписан электронной подписью лица, которое указано в тексте электронного документа как лицо, его подписавшее. Подача документов в электронном виде, в том числе в форме электронного документа, происходит через личный кабинет и требует приложения документа, подтверждающего полномочия представителя.

Процесс ведения электронного делопроизводства представляет собой сложную систему, включающую

совокупность разнородных данных, обрабатываемых с использованием информационных систем, где на различных этапах их обработки присутствует человеческий фактор, что существенно влияет на достоверность, законность и необратимость действий при операциях с юридически значимыми документами. Набор разнообразных источников данных и электронных документов и участие в процессах различных сторон предъявляют высокие требования к качеству информации. Процесс обработки информации в подобных системах включает операции ввода, экспорта, импорта, обмена, предобработки, анализа, вывода, кодирования, шифрования и др. Данные операции в большинстве своем могут быть включены в состав функциональных возможностей правовой информационной системы. При этом качество судебных документов определяется точностью, достоверностью, полнотой и непротиворечивостью, при необходимости — соблюдением *конфиденциальности* и *секретности* [4].

Предлагаемый подход к созданию как корпоративной, так и открытой блокчейн-сети позволит создать информационную систему на основе безотказной связности сети с постоянной топологией и скоростью передачи информации. Сетевая структура информационной системы по технологии блокчейн является безопасной, так как трафик в сети не может быть модифицирован третьей стороной (рис. 1). Централизованное администрирование и идентичность узлов и линий связи основано на универсальной для всей сети системе отсчета времени.

Построение сети с ограниченным объемом узлов позволяет минимизировать время передачи транзакций в распределенной базе данных. Ориентировочная оценка временных характеристик доступа к реестру данных одноранговой сети, к которой относится блокчейн-сеть, позволяет оценить доступность узлов сети с заданными параметрами на основе существующей организационной структуры судебной системы.

Важное преимущество хранения данных на платформе распределенного реестра — высокая надежность, исключающая возможность потери или уничтожения. Принципиальная открытость данных, простота доступа и проверки правовых данных устраняют возможность совершения коррупционных сделок в ходе судебного процесса. Сокращаются издержки на ведение реестров, повышается оперативность предоставления данных потребителям.

Основные *вероятностно-временные характеристики* информационной коммуникационной блокчейн-сети с синхронным временным доступом при массовом обслуживании пользователей включают следующие показатели:

$$\langle V_c, D, R_c, Q, T_{\text{бл}} \rangle,$$

где V_c — скорость передачи данных в сети; D — доступность узлов сети; R_c — скорость передачи данных блока в сети; Q — вероятность включения блока в цепочку; $T_{\text{бл}}$ — среднее время создания блоков данных в цепочке блокчейн.

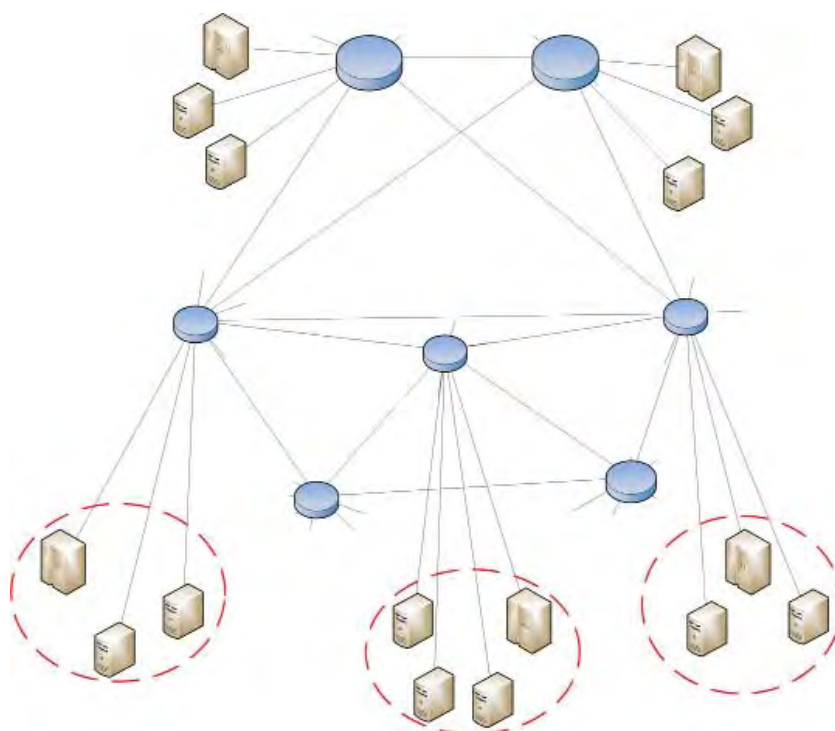


Рис. 1 Функциональные уровни информационной сети распределенного реестра

Если предполагаемая одноранговая сеть характеризуется графом без циклических структур, где N_d — число узлов сети на расстоянии d ; n — полное число участников в сети; d — расстояние между узлами блокчейн-сети, тогда доступность D узлов сети с учетом количества узлов сети и связей между узлами блокчейн-сети можно определить из выражения:

$$D = \sum_{d=1}^n \frac{dN_d}{N-1}.$$

Информационная скорость взаимодействия узлов с учетом создания цепочки блоков в сети $R_c^{\text{бл}} = R_c Q$, бум/с ; информационная скорость одноранговой сети $R_c = \lambda k N$, бум/с и интенсивность потока транзакций в блокчейн-сети $\Lambda = \lambda N$ позволяют рассчитать вероятность Q :

$$Q = W(s)B(s),$$

где $s = 1/T_{\text{бл}}$; $W(s) = \frac{s(1-\rho)}{s - \lambda + \lambda B(s)}$ — функция распределения времени ожидания для транзакций в сети; $\rho = \lambda(N-1)T_{\text{бл}}$.

Время ожидания завершения транзакции, исходя из преобразования Лапласа для фиксированного времени формирования блоков, носит экспоненциальный характер:

$$B(s) = e^{-s(N-1)T_{\text{бл}}},$$

где $B(s)$ — преобразование Лапласа для функции плотности равномерного распределения вероятностей.

Среднее время $T_{\text{бл}}$ создания блоков данных в цепочке блокчейн с учетом скорости V_c передачи данных в сети и интенсивности Λ потока транзакций:

$$T_{\text{бл}} = t_{\text{прд}} + t_{\text{пдт}} + t_{\text{тр}} + t_{\text{бл}},$$

где $t_{\text{прд}} = \frac{D}{0,7c}$ — время передачи блока в сети;

$c = 3 \cdot 10^8$ м/с; $t_{\text{пдт}} = \frac{n_{\text{пдт}}}{V_c}$ — время подтверждения

создания блока; $t_{\text{тр}} = \frac{d[W(s)B(s)]}{ds}$ — требуемое вре-

мя доставки блока; $t_{\text{бл}} = \frac{n_k}{V_c}$ — время создания блока.

Система распределенных баз данных, лежащая в основе технологии блокчейн, состоит из набора узлов (*site*), связанных коммуникационной сетью, в которой каждый узел — это полноценная система управления базой данных. Все узлы взаимодействуют между собой таким образом, что пользователь любого из них может получить доступ к любым данным в сети так, как будто они находятся на его собственном узле. Локальные данные хранятся в соответствии с их структурной принадлежностью, а к удаленным данным доступ осуществляется по мере необходимости [3].

При решении задачи аутентификации источника данных не доверяющих друг другу сторон применяют технологию *электронной подписи* [5], позволяющую осуществлять аутентификацию источника данных по алгоритмам шифрования ГОСТа, возможно, на ближайшую перспективу с *гарантированной* безопасностью.

Использование российских сертифицированных алгоритмов криптографической защиты информации позволяет придать юридическую значимость доку-

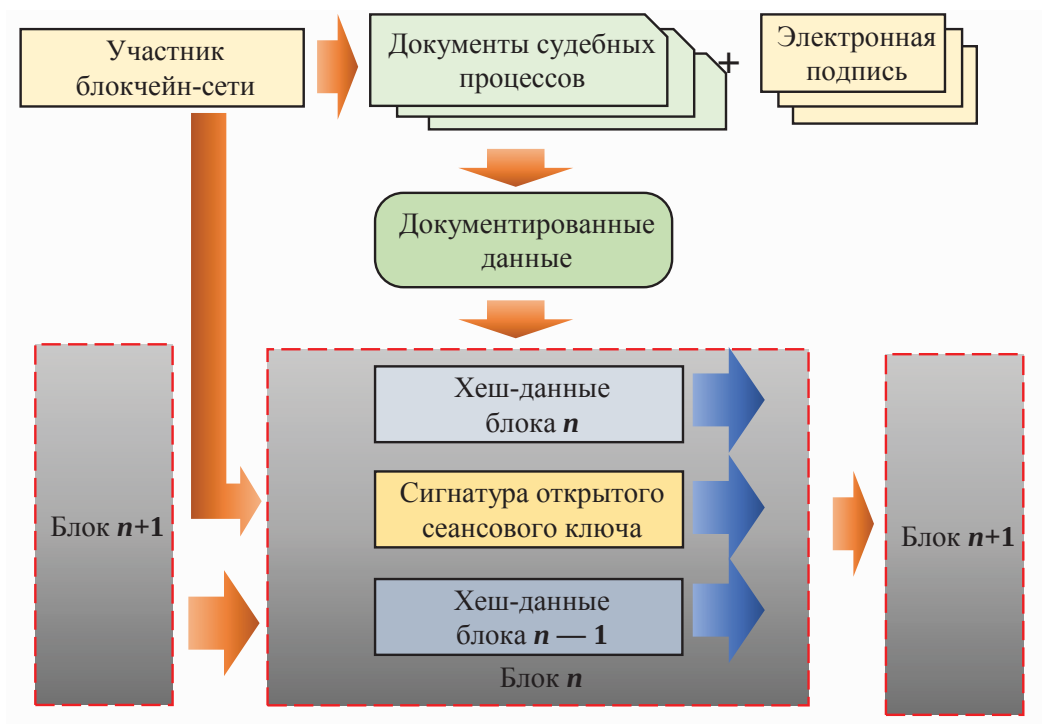


Рис. 2. Структура блока документов

ментальным данным судебного процесса через соответствие законодательству Российской Федерации, в частности, Федеральному закону от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и криптографическим преобразованиям, реализуемым средствами криптографической защиты информации (СКЗИ), имеющим соответствующую сертификацию в РФ.

В информационной системе, построенной с использованием криптографических технологий, хэш-функции имеют разнообразное применение: при проверке целостности записей в базах данных, построении алгоритмов быстрого поиска, проведении статистических экспериментов, тестировании логических устройств и др. В современных системах управления базами данных при осуществлении поиска нужных данных в большом объеме информации различного содержания сравниваются друг с другом не сами данные, а короткие значения их сверток, одновременно являющиеся контрольными суммами. Основным требованием к хэш-функциям является равномерность распределения их значений при случайном выборе значений аргументов. В данном случае хэш-функция не зависит от секретного ключа и может быть фиксирована и известна всем. Это дает гарантии невозможности подмены подписанного документа, а также подбора двух различных сообщений с одинаковым значением хэш-функции (в таких случаях говорят, что пара информационных массивов образует коллизию) [14].

Способы построения записей в цепочке не требуют использования публичной криптографии. Использование хэш-функций обеспечивает достаточную степень

защиты информации, что обеспечивает доверие к технологии. При решении задачи аутентификации источника данных не доверяющих друг другу сторон используется технология электронной подписи, позволяющей осуществлять аутентификацию источника данных. При этом сообщение должно быть подписано личной подписью, основанной на секретном ключе пользователя.

Алгоритм работы системы кодирования заключается в добавлении специального префикса и вычислении контрольной суммы путем хеширования полученной последовательности данных. Результатом хеширования является n -байтный дайджест (рис. 2).

Стойкость алгоритма шифрования в блокчейн-сети определяется стойкостью формируемого секретного ключа, так как открытый ключ является общедоступной информацией. Считается, что стойкость ключевой криптографической информации определяется временем, необходимым для вскрытия всех его символов; соответственно, чем больше время вскрытия секретного ключа, тем больше его стойкость. Если предположить, что решение задачи по вскрытию ключевой криптографической информации осуществляется на вычислительном кластере проекта TOP-500, имеющего максимальную суммарную вычислительную мощность $G = 93014,6$ TFlop/s (вычислительная мощность суперкомпьютеров рейтинга TOP-500), это позволяет обеспечить на интервале в течение суток (24 ч) невскрытие ключевой криптографической информации через 10—15 лет [12].

К технологии блокчейн в мире проявляют интерес представители различных сфер. Степень заинтересованности государственных органов и частных ком-

паний в разных секторах экономики и общественной жизни значительно отличается. Активно используются и повсеместно внедряются технологии блокчейн в финансовом секторе, но при этом государственные учреждения и производственные предприятия уделяют данной технологии недостаточно внимания. Блокчейн как технология до недавнего времени не попадала под нормативное регулирование и сертифицировать можно было только решения, созданные с помощью данной технологии. По результатам экспертизы 7 октября 2019 г. было получено положительное заключение ФСБ России для блокчейн-платформы Мастерчейн², разработанной Ассоциацией ФинТех (АФТ)³. Мастерчейн стал первой сертифицированной платформой, которая использует российские стандарты криптографии и соответствует требованиям информационной безопасности.

Блокчейн представляет собой технологию распределенного реестра на основе децентрализованной базы данных, для управления которой используются криптографические методы защиты информации. Данная технология лежит в основе работы криптовалют, в том числе таких, как *Bitcoin*, *Ethereum*, *Litecoin*, *Dogecoin*, *Zcash* и др. Главное свойство блокчейн-сети — неизменяемость или очень трудная, практически невозможная обратимость созданной цепочки блоков данных. Внесенные в базу данных сведения о сделке (транзакции) нельзя удалить, отредактировать, так как даже незначительная правка требует огромных вычислительных ресурсов, поскольку реестр с информацией хранится в распределенной базе данных и постоянно обновляется в сети с учетом временных параметров [11].

Для удовлетворения возникших потребностей необходима разработка новых качественных сервисов, позволяющих участникам судебных процессов: подавать в суд заявления и ходатайства, получать своевременно уведомления, извещения, повестки, работать с электронными судебными документами, иметь доступ к информационным ресурсам суда с различных устройств и из любого места. *Информационное пространство судебной системы* представляется в виде распределенной структуры, основу которой определяют модели гражданского, уголовного, административного, арбитражного процессов, а также порядок рассмотрения дел об административных правонарушениях [7].

С этой целью подлежит первоочередной целенаправленной модернизации программное обеспечение существующей и развивающейся Государственной автоматизированной системы (ГАС) РФ «Правосудие», имеющее в своем составе программные изделия «Банк судебных решений (судебной практики)» и «Судимость» (функциональная подсистема «Судебное делопроиз-

водство и статистика») для выполнения аналитических задач судебной статистики, и программное изделие «Документооборот» (подсистема «Документооборот и обращения граждан»), обеспечивающее представление информации и организации унифицированного доступа к распределенным информационным хранилищам. Постоянный рост объема документов в судебной сфере при дефиците помещений, предназначенных для хранения архивов, а также несоответствии имеющихся площадей архивов нормам хранения документов и требованиям пожарной безопасности постоянно требует немалых финансовых затрат [8, 9, 13]. Также нуждается в существенной доработке концепция подготовки квалифицированных специалистов [2], способных обеспечить правовое регулирование в сфере функционирования судебной информационной системы документооборота на блокчейн-платформе, решения задачи обеспечения открытости сервиса для пользователей и поддержания высокой степени защищенности документальных данных всех участников судебного процесса на всем его протяжении.

Использование технологии блокчейн в судопроизводстве — в первую очередь инструмент формирования среды доверия участников судебных споров и только потом средство хранения и представления информации. Сеть, построенная по технологии блокчейн, представляет собой инструмент для устранения недоверия сторон в сфере судебного делопроизводства. При этом в качестве дополнительных сервисов обеспечивается пространственно-временной континуум и механизм комплексной проверки документов профессиональными экспертами.

Применение технологии блокчейн позволяет свести к минимуму множество дорогостоящих и длительных юридических процедур, а также количество участников, имеющих отношение к ведению судебных споров. Использование подобной технологии дает возможность отслеживать движение судебных дел, историю документов и договоренностей в сфере судопроизводства, а также организовать оборот юридически значимых документов по принципу транзакции, при этом алгоритм взаимодействия обеспечивает то, что ни одна из сторон не сможет обмануть другую. Такие решения, исключая человеческий фактор из системы оборота и контроля судебных документов, сводят к минимуму коррупционную составляющую в них.

Реализация технологии блокчейн позволит сформировать единый стандарт применения технологии в государственном управлении и при оказании государственных услуг [16]. Преимущества рассматриваемого подхода в организации процессов судопроизводства очевидны как для населения страны, так и для государства и его судебной системы. Данный подход позволит:

- оптимизировать время оформления комплекта документов;
- исключить необходимость обращаться повторно в судебные органы; документы не могут быть утеряны, изменены или повреждены;

² Децентрализованная сеть обмена и хранения информации «Мастерчейн», версия 1.1 // Интернет-портал TAdviser 2019. URL: http://www.tadviser.ru/images/a/ad/Masterchain_whitepaper_11_08.pdf (дата обращения: 26.06.2020).

³ Ассоциация «ФинТех» основана в конце 2016 г. по инициативе Банка России и ключевых участников российского финансового рынка.

- обеспечить быструю проверку состояния и статуса документов;
- снизить коррупционную составляющую в судебных спорах.

Возможности технологии доступны для реализации вследствие простоты концептуальной и практической проверки правильности работы информационной системы, что, в свою очередь, ведет к увеличению доверия к создаваемой *системе судебного документооборота*. Сервисы услуг сети по обработке данных транзакций, построенные по технологии блокчейн, позволяют создавать записи распределенного реестра в рамках судебных процессов, включающие необходимый набор документальной, правовой информации всех участников судебных споров. Сервисы могут быть как экстерриториальными, так и локальными, т. е. поддерживаться определенной организацией, имеющей распределенную структуру, или быть сосредоточенными на одном вычислительном ресурсе, принадлежащем нескольким структурам. Обработываемые сервисом данные могут быть закрытыми или открытыми, анонимными или персонифицированными, в зависимости от решаемых системой задач [15].

Построенные на основе этой технологии сервисы для ведения реестров реализованы в виде распределенной базы данных, развернутой в пространстве на системе серверного оборудования, принадлежащего государственной структуре, представленной полными узлами (узел консенсуса), узлами аудита и конечными, клиентскими узлами (см. рис. 1). Это позволяет использовать существующую организационную структуру судебной системы. Работа системы предоставления услуг по технологии блокчейн основана на согласованной работе серверов по предоставлению индивидуального открытого ключа для взаимодействия пользователей в блокчейн-сети. Каждый сервер имеет копию базы данных, которая используется при обработке транзакций и в реестр которой вносятся записи. Изменение копии на локальных узлах распределенной сети приводит к изменению в базе данных на других серверных узлах. Высокая степень дублирования информации, наличие механизмов автоматического перестроения сети и восстановления ее после сбоев в работе обеспечивают высокую степень надежности предоставляемых услуг [3].

Согласование принципов взаимодействия между сторонами, участвующими в правовых процессах, основано на использовании алгоритмов доверия (консенсуса) взаимодействующих сторон. Консенсус между сторонами, не доверяющими друг другу, — это набор определенных математических правил и законов, которые регулируют работу по созданию цепочки блоков. Решение данной задачи в настоящее время основано на сложных вычислениях математической функции и требует больших вычислительных мощностей. Полученные решения могут быть быстро проверены и используются для создания блоков в цепи блокчейн. Самыми используемыми в информационных системах на основе блокчейн-технологии являются два алгоритма:

Proof-of-Work («доказательство работы») и *Proof-of-Stake* («доказательство доли владения»). Также существуют и другие, однако они представлены в намного меньшем количестве решений на основе блокчейн-технологии. Это связано в первую очередь с их относительно недавним появлением и недостаточно отработанной технологией применения.

Уникальный цифровой идентификатор, используемый в распределенных базах данных по технологии блокчейн, и связанную с ним последовательность записей иногда называют «токеном» (от англ. *token* — жетон, маркер). Токены создаются и распределяются в сети блокчейн узлами сети с высокой вычислительной мощностью и имеют определенную ценность. Данные узлы должны принадлежать административным структурам или быть сертифицированы. Передача данных токенов участникам транзакции дает возможность добавления очередного блока в цепочку записей [11].

Используемый метод связывания гарантирует невозможность скрытого изменения как данных в блоке, так и замены самого блока в цепочке. Невозможно также нарушение истории совершения транзакций в рамках судебного спора или подмены текущего владельца токена без его ведома, а это все представители правовой системы государства и остальные участники судебного процесса. Высокие показатели защищенности данных в системе достигаются обеспечением *конфиденциальности, сохранности и достоверности* информации [5]. Распределенная база данных и децентрализованная сеть серверов ведут к многократному дублированию информации и высокой степени надежности работы системы. Понятие транзакции давно применяется в банковской сфере, биржевой торговле. В блокчейн-технологии под транзакцией понимают минимальную логически операцию, которая имеет смысл и может быть совершена только полностью. Транзакция или *смарт-контракт* (умный контракт) в правовых процессах предусматривает набор процедур определенной последовательности, совершаемых при действиях с правовой документацией всех участников судебных процессов [10, 11].

Информация, хранящаяся в распределенной базе сети блокчейн, не является секретной. Необходимости во взломе базы нет, и нарушителю это не даст ничего, что он не мог бы получить, пользуясь стандартными правилами доступа. Это значительно уменьшает заинтересованность во взломе сервера. Это свойство может быть использовано для проведения транзакций между сторонами, которые не полностью доверяют друг другу. Сервисы, использующие правила взаимодействия сторон, не известных друг другу, необходимы при проведении сделок с недвижимостью, для владельцев акций, соблюдении прав и требований кредиторов, учета автотранспорта или любого другого имущества, сделок, контрактов, обязательств, обременений и так далее.

С правовой точки зрения участники информационного взаимодействия с применением технологии блок-

чейн должны принимать на себя ряд обязательств, где должно быть четко указано [17]:

- кто должен нести ответственность в случае, если правовые данные не соответствуют требованиям судебного процесса;
- кто должен нести ответственность в случае, если система окажется ненадежной и будет выявлен факт нарушения данных в блокчейн-сети;
- какова ответственность стороны, допустившей нарушения в правовых документах, приведшие к аннулированию транзакции;
- какова ответственность владельца узла сети блокчейн в случае его дискретизации;
- кто несет материальную ответственность за нарушения на этапах совершения транзакции и обеспечение сервисных услуг;
- каков порядок разрешения коллизий и споров в случае нарушения правил судебного делопроизводства.

Поскольку данные проблемы носят юридический, а не технический характер, то для их разрешения необходимо заключение юридически обоснованных договоров. Оформление договора является стандартной процедурой для каждой стороны, участвующей в совершении процессуальных действий в судебных спорах.

При переходе на электронную регистрацию документов, на ведение электронных реестров, на взаимодействие участников судебного процесса преимущественно в электронной форме необходимо говорить о том, что наибольшая уязвимость системы существует в рамках идентификации и аутентификации заявителя и остальных участников судебных споров. Проведение идентификации и аутентификации необходимо по нескольким параметрам, когда голос, лицо и отпечаток пальцев одновременно уже используются для подтверждения личности участников совершения транзакции. На сегодня в законодательных органах находятся на рассмотрении правовые акты, определяющие возможность перехода на идентификацию личности по трем биологическим параметрам [6] при совершении запросов и подаче пакетов документов для реализации своих требований в электронной форме.

Судебная система Российской Федерации, являясь независимым элементом государственной власти, нуждается в оптимизации сферы правовых отношений на

основе соблюдения баланса интересов, взаимной ответственности и скоординированных усилий государства, общества и населения. Переход к инновационному, базирующемуся на принципах новых информационных технологий и социально ориентированному типу информатизации процессов правосудия и самой судебной системы сегодня является одним из наиболее актуальных направлений развития инфраструктуры государства.

Первые шаги в области цифровизации судебной деятельности предприняты судом по интеллектуальным правам. Некоммерческая организация «Ассоциация *IPChain*», созданная по инициативе ряда фондов и компаний, таких как Фонд развития Центра разработки и коммерциализации новых технологий (г. Сколково), Общество по коллективному управлению смежными правами «Всероссийская организация интеллектуальной собственности» (ВОИС) и др., развернула децентрализованную сеть транзакций с правами и объектами интеллектуальной собственности *IPChain*. Судом по интеллектуальным правам РФ создан узел блокчейн-сети *IPChain*, что позволило российской судебной системе практически размещать транзакции по результатам судебных решений об изменении состава правообладателей на объекты интеллектуальной собственности в блокчейн-сети «*IPChain*». В данном конкретном случае используются возможности блокчейн-технологии по гарантированному сохранению неизменности результатов судебного спора.

Таким образом, применение рассмотренного подхода для решения задач учетно-регистрационной деятельности в сфере правосудия позволит не только сохранить накопленный потенциал и привести к созданию информационной системы на базе реестра достоверных данных правовых споров, гармонизации сферы правосудия в целях повышения эффективности судебных споров, защиты прав участников процессов и снижения административных барьеров, но и позволит повысить место Российской Федерации в рейтинге, который составляется по Индексу развития информационно-коммуникационных технологий стран (ИКТ) — *ICT Development Index, (IDI)*, одному из ключевых индикаторов развития информационного общества в странах мира.

Литература

1. Ващекин А. Н., Дзедзинский А. В. Проблемы правового регулирования отношений в цифровом пространстве // Правосудие. 2020. Т. 2. № 2. С. 126—147. DOI: 10.37399/issn2686-9241.2020.2-126-147.
2. Ершов В. В., Ловцов Д. А. Концепция непрерывной информационной подготовки юриста // Информационное право. 2007. № 3. С. 29—34.
3. Дейт К. Дж. Введение в системы баз данных. М. : Изд. дом «Вильямс», 2005. 1328 с. ISBN 5-8459-0788-8.
4. Ловцов Д. А. Проблемы правового регулирования электронного документооборота // Информационное право. 2005. № 2. С. 28—31.
5. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: Монография. М. : Росс. гос. ун-т правосудия, 2016. 316 с. ISBN 978-5-93916-505-1.
6. Ловцов Д. А., Князев К. В. Защищенная биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100—103.

7. Ловцов Д. А., Ниесов В. А. Формирование единого информационного пространства судебной системы России // Российское правосудие. 2008. № 11. С. 78—88.
8. Ловцов Д. А., Ниесов В. А. Проблемы и принципы системной модернизации «цифрового» судопроизводства / Правовая информатика. 2018. № 2. С. 15—22. DOI: 10.21681/1994-1404-2018-2-15-22.
9. Ловцов Д. А., Черных А. М. Геоинформационные системы. М. : Росс. акад. правосудия, 2012. 188 с. ISBN 978-5-93916-340-8.
10. Савельев А. И. Некоторые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. С. 94—117.
11. Свон М. Блокчейн: Схема новой экономики. М. : Олимп-Бизнес, 2017. 240 с.
12. Тутубалин П. И., Кирпичников А. П. Оценка криптографической стойкости алгоритмов асимметричного шифрования // Вестник Технологического университета. 2017. Т. 20. № 10. С. 94—99.
13. Федосеев С. В. Применение современных технологий больших данных в правовой сфере // Правовая информатика. 2018. № 4. С. 50—58. DOI: 10.21681/1994-1404-2018-4-50-58.
14. Фергюсон Н., Шнайер Б. Практическая криптография. М. : Изд. дом «Вильямс», 2005. 420 с.
15. Черных А.М. Защищенность данных об объектах недвижимости и земельных ресурсах на базе геоинформационных систем и технологии блокчейн // Правовая информатика. 2019. № 4. С. 75—85. DOI: 10.21681/1994-1404-2019-4-75-85.
16. 1Franco P. The Blockchain // Understanding Bitcoin: Cryptography, Engineering and Economics. John Wiley & Sons, 2014. 288 p. ISBN 978-1-119-01916-9.
17. Madnick S. Blockchain is unbreakable? Think again // The Wall Street Journal. 2019. 6 june. URL: <http://blogs.wsj.com/experts/2019/> (дата обращения 10.10.2020).

Рецензент: **Бетанов Владимир Вадимович**, доктор технических наук, профессор, член-корреспондент Российской академии ракетных и артиллерийских наук, заместитель начальника центра АО «Российские космические системы», Российская Федерация, г. Москва.

E-mail: vlavab@mail.ru

DISTRIBUTED REGISTER TECHNOLOGIES AND PROTECTING THE JUDICIAL DOCUMENTS FLOW SYSTEM

Andrei Chernykh, Ph.D. (Technology), Associate Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.

E-mail: kafpi@mail.ru

Keywords: *judicial system, document flow, blockchain network, blockchain technology, electronic record keeping, distributed database, database management system, hash functions, network encryption algorithm.*

Abstract.

Purpose of the work: *justifying the possibility of creating a judicial documents flow information system on the blockchain platform, solving the problem of ensuring the openness of this service for users, and maintaining a high degree of protection of documentary data of all participants of court proceedings throughout its entire course.*

Methods used: *informational and structural analysis of judicial documents from the standpoint of a distributed telecommunications network built using blockchain technology with a view to solve problems of reliable document flow during court proceedings considering ensuring a consensus of interested parties and the impossibility of making changes to the documents used in the proceedings without the consent of all participants.*

Results obtained: *a justification is given for the possibility of using blockchain technology in constructing a information system for court proceedings, a transition to electronic documents registration and maintaining electronic registers in the interaction of participants of court proceedings predominantly in electronic form are considered, a logical conceptual model of document flow during court proceedings is developed using a distributed register with a high degree of information protection over a long period of time ensuring a reduction of the corruption component in the control and inventory management system for legally authentic documents of court proceedings.*

References

1. Vashchekin A. N., Dzedzinskii A. V. Problemy pravovogo regulirovaniia otnoshenii v tsifrovom prostranstve. *Pravosudie*, 2020, t. 2, No. 2, pp. 126-147. DOI: 10.37399/issn2686-9241.2020.2-126-147.
2. Ershov V. V., Lovtsov D. A. Kontsepsiia nepreryvnoi informatsionnoi podgotovki iurista. *Informatsionnoe pravo*, 2007, No. 3, pp. 29-34.
3. Deit K. Dzh. Vvedenie v sistemy baz dannykh. M. : Izd. dom "Vil'iams", 2005, 1328 pp. ISBN 5-8459-0788-8.
4. Lovtsov D. A. Problemy pravovogo regulirovaniia elektronnoho dokumentooborota. *Informatsionnoe pravo*, 2005, No. 2, pp. 28-31.
5. Lovtsov D. A. Sistemologiya pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere: Monografiia. M. : Ross. gos. un-t pravosudiia, 2016, 316 pp. ISBN 978-5-93916-505-1.
6. Lovtsov D. A., Kniazev K. V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolya dostupa. I. Matematicheskie modeli i algoritmy. *Informatsiia i kosmos*, 2013, No. 1, pp. 100-103.
7. Lovtsov D. A., Niesov V. A. Formirovanie edinogo informatsionnogo prostranstva sudebnoi sistemy Rossii. *Rossiiskoe pravosudie*, 2008, No. 11, pp. 78-88.
8. Lovtsov D. A., Niesov V. A. Problemy i printsipy sistemnoi modernizatsii "tsifrovogo" sudoproizvodstva. *Pravovaia informatika*, 2018, No. 2, pp. 15-22. DOI: 10.21681/1994-1404-2018-2-15-22.
9. Lovtsov D. A., Chernykh A. M. Geoinformatsionnye sistemy. M. : Ross. akad. pravosudiia, 2012, 188 pp. ISBN 978-5-93916-340-8.
10. Savel'ev A. I. Nekotorye aspekty ispol'zovaniia smart-kontraktov i blokchein-tekhnologii po rossiiskomu pravu. *Zakon*, 2017, No. 5, pp. 94-117.
11. Svon M. Blokchein: Skhema novoi ekonomiki. M. : Olimp-Biznes, 2017, 240 pp.
12. Tutubalin P. I., Kirpichnikov A. P. Otsenka kriptograficheskoi stoikosti algoritmov asimmetrichnogo shifrovaniia. *Vestnik Tekhnologicheskogo universiteta*, 2017, t. 20, No. 10, pp. 94-99.
13. Fedoseev S. V. Primenenie sovremennykh tekhnologii bol'shikh dannykh v pravovoi sfere. *Pravovaia informatika*, 2018, No. 4, pp. 50-58. DOI: 10.21681/1994-1404-2018-4-50-58.
14. Fergiuson N., Shnaier B. Prakticheskaya kriptografiia. M. : Izd. dom "Vil'iams", 2005, 420 pp.
15. Chernykh A. M. Zashchishchennost' dannykh ob ob'ektakh nedvizhimosti i zemel'nykh resursakh na baze geoinformatsionnykh sistem i tekhnologii blokchein. *Pravovaia informatika*, 2019, No. 4, pp. 75-85. DOI: 10.21681/1994-1404-2019-4-75-85.
16. Franco P. The Blockchain. Understanding Bitcoin: Cryptography, Engineering and Economics. John Wiley & Sons, 2014, 288 p. ISBN 978-1-119-01916-9.
17. Madnick S. Blockchain is unbreakable? Think again. *The Wall Street Journal*, 6 june 2019. URL: <http://blogs.wsj.com/experts/2019/> (data obrashcheniia 10.10.2020).