НАУЧНАЯ СТАТЬЯ
УДК 656.7:621:004.056
DOI: https://doi.org/10.30932/1992-3252-2024-22-4-4

Мир транспорта. 2024. Т. 22. № 4 (113). С. 27–32

Анализ работы распределенного реестра данных на примере аэропорта

Игорь РОЗЕНБЕРГ

Яков ДАЛИНГЕР

Игорь Наумович Розенберг [1]**,**
Яков Михайлович Далингер [2]

[1, 2] *Российский университет транспорта, Москва, Россия.*
[1] *ORCID: https://orcid.org/0000-0001-9589-6783; Web of Science Researcher ID: AAD-7632-2019; Scopus Author ID: 15136568900; РИНЦ SPIN-код: 2958-4186; РИНЦ Author ID: 652172.*
[2] *ORCID: https://orcid.org/0000-0002-7744-7156; Web of Science Researcher ID: B-6790-2019; Scopus Author ID: 57195278185; РИНЦ SPIN-код: 8895-3700; РИНЦ Author ID: 704687.*
✉ [2] *iakovdalinger@gmail.com.*

АННОТАЦИЯ

Показаны возможности применения технологии распределенного реестра для хранения данных в информационных системах аэропортов и авиационных систем различного уровня.

Отмечены особенности работы распределенного реестра в информационных системах. Исследованы различные варианты формирования сообщений для хранения в распределенном реестре и параметры потоков сообщений. Выделены особенности применения технологии блокчейн при создании распределенных реестров в случае необходимости коррекции хранимой информации.

Показаны возможности применения сетевых технологий при формировании распределенных реестров, узлы которых находятся на значительных расстояниях друг от друга (реестры нескольких аэропортов).

Представленные данные могут применяться при создании надежных распределенных хранилищ информации, как в рамках отдельного аэропорта, так и для группы аэропортов.

Ключевые слова: распределенная информационная система, распределенный реестр, блокчейн, информационная безопасность, криптозащита, математические модели, гражданская авиация, аэропорты.

Для цитирования: Розенберг И. Н., Далингер Я. М. Анализ работы распределенного реестра данных на примере аэропорта // Мир транспорта. 2024. Т. 22. № 4 (113). С. 27–32. DOI: https://doi.org/10.30932/1992-3252-2024-22-4-4.

Полный текст статьи в переводе на английский язык публикуется во второй части данного выпуска.
English translation of the full text of the article is published in the second part of the issue.

ВВЕДЕНИЕ

Технология распределенных реестров (часто, технология на базе блокчейн) становится все более популярной при создании распределенных информационных систем ввиду таких ее особенностей, как [1–6]:

• распределенное хранение копий, позволяющее осуществлять одновременный доступ к реестру многих пользователей в различных географических точках;

• невозможность внесения несанкционированных изменений в созданные копии;

• высокая функциональная надежность реестра;

• возможность управления доступом к копиям реестра;

• когерентность (полное соответствие) копий реестра;

• возможность неограниченного наращивания содержимого реестра.

Это позволяет применять технологию распределенных реестров для построения специализированных информационных систем предприятий и их объединений на региональном и федеральном уровнях [1].

Процесс создания специализированных информационных систем на базе распределенных реестров и их эксплуатация значительно отличаются от методов создания и эксплуатации систем, связанных с криптовалютой, что необходимо учитывать при проведении разработок.

Основные отличия состоят в следующем:

• Отсутствие майнинга, связанного с необходимостью конкурировать за право занесения данных в реестр и вознаграждение.

• Территориальная локализация копий распределенного реестра (например, в пределах региона, государства и т. д.).

• Соблюдение законодательных, отраслевых и прочих нормативов, регламентирующих обработку и доступ к информации.

• Необходимость обеспечения защиты информации от специфических угроз, связанных с функционированием реестра, свойствами хранимой информации управлением доступом (решение задач кибербезопасности).

• Необходимость обеспечения доступа к реестру большого числа пользователей (администраторы, осуществляющие ведение реестра; пользователи, обращающиеся с запросами к реестру).

• Наличие специальных средств проверки (валидации) данных, заносимых в реестр, в зависимости от назначения данных.

• Наличие криптографических средств защиты данных (шифрование, хэширование, аутентификация) [7–11].

Кроме того, копии реестра содержат большое количество различной информации, структурированной в виде блоков, что требует создания средств ее поиска и представления в удобном для пользователей виде (база данных реестра).

Все это обуславливает целесообразность создания методов анализа вариантов распределенного реестра, обусловленных спецификой его практического применения.

Среди задач организации важное место занимают задачи формирования потока блоков данных для записи в реестр.

Целью исследования является анализ возможности применения технологии распределенного реестра при создании распределенных баз данных информационных систем аэропортов и авиапредприятий различного уровня.

В исследовании были использованы *методы* системного анализа, теории очередей, теории вероятностей, теории компьютерных сетей и информационных систем.

РЕЗУЛЬТАТЫ

Описание реестра

Распределенный реестр целесообразно создавать как развитие интегрированных распределенных баз данных, когда имеется совокупность информационных ресурсов с установленными связями, системой запросов и обновлений [12]. Возможный вариант организации распределенного реестра рассмотрен для случая транспортного предприятия, например аэропорта, со следующими характеристиками:

1. Распределенный реестр создается на базе имеющихся информационных ресурсов и состоит из группы локальных реестров отдельных подразделений аэропортов.

2. Все локальные реестры могут создаваться в виде блокчейнов – специальных

[1] Спиркина А. В. Разработка модели применения систем распределенного реестра и оценки их влияния на сетевые характеристики / Дисс… канд. техн. наук. – СПб.: СПбГУТ, 2022. – 186 с.

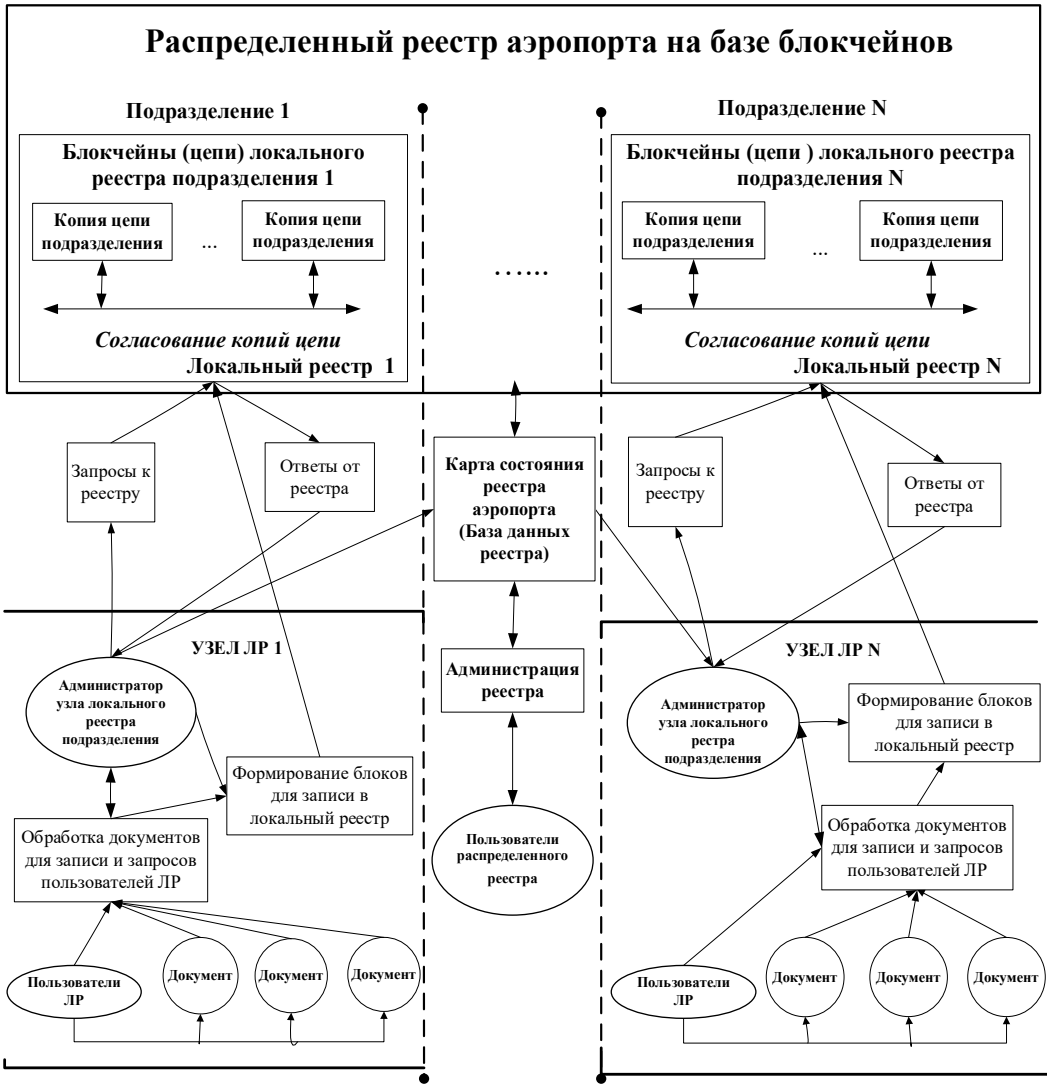

Рис. 1. Обобщенная структура распределенного реестра аэропорта [составлена авторами].

цепочек данных, обладающих свойствами, перечисленными выше [1; 2; 6; 11].

3. Технологию блокчейн целесообразно применять для случаев, когда имеются повышенные требования к безопасности данных, однако при этом возникают значительные сложности с внесением изменений в хранимые данные.

4. Каждый локальный реестр создается для одного или нескольких подразделений аэропорта, информация локальных реестров может пересекаться.

5. Для внесения записей (блоков) в локальные реестры выделяются специальные рабочие места с соответствующим программным обеспечением, позволяющим проводить валидацию и согласование данных.

6. Копии локальных реестров доступны сотрудникам – администраторам реестров соответствующих подразделений, которые обеспечивают их заполнение и работу с реестрами по запросам сотрудников аэропорта и внешних организаций (пользователей реестра).

7. Распределенный реестр содержит карту локальных реестров (базу данных реестра), где формируются данные для доступа к локальным реестрам по запросам.

Работа с реестром состоит из формирования блоков документов для записи, записи блоков и копий в локальные реестры,

обработки запросов к реестру (поиск требуемой информации, представление найденной информации в требуемой форме). Сформированные для записи блоки проходят проверку (валидацию) на отсутствие копий, правильность записи и после успешной проверки записываются по установленным правилам в локальный реестр (блокчейн) соответствующего подразделения.

Пример варианта обобщенной структуры распределенного реестра аэропорта приведен на рис. 1. В данном случае локальные реестры созданы с применением технологии блокчейн.

Возможно масштабирование структуры для авиатранспортной системы, включающей несколько авиационных и вспомогательных (обслуживающих) предприятий.

Сотрудники – администраторы локальных реестров имеют право формировать блоки документов для записи в свои реестры, обрабатывать запросы к реестрам.

Блоки состоят из конечного числа документов, которые обрабатываются в данном подразделении.

Каждый администратор формирует блоки из заданного множества доступных ему документов так, что блоки разных администраторов не содержат одинаковых документов.

Документы могут образовываться в процессе работы подразделения либо поступать из внешних подразделений или организаций [13].

Перед записью созданного блока в локальный реестр проводится его валидация, которая заключается в проверке корректности документов, проверке отсутствия одинаковых документов в разных блоках, проверке корректности записи данных о владельце (создателе) блока.

Для валидации созданный блок рассылается всем сотрудникам – администраторам локального реестра. Администратор, получивший блок, проводит его проверку и высылает ответ с результатами проверки в адрес администратора, создавшего блок [13].

Если все ответы собраны и все они положительны, администратор, создавший блок, проводит его запись в свою копию локального реестра.

Если несколько администраторов работают с одной копией, то запись происходит в установленном для них порядке без розыгрыша права записи.

В заданные моменты времени происходит согласование копий локального реестра.

Возможны уточнения работы, связанные со спецификой предприятия, например, применение шифрования документов, распределение ключей для обработки блоков и документов, установление специальных правил ведения и согласования копий локального реестра.

Для обеспечения поиска документов в пределах всего распределенного реестра составляется карта локальных реестров учреждения. Карта представляет специализированную базу данных, где хранится информация о размещении документов, данные о владельцах блоков, данные для формирования запросов к локальным реестрам.

Для создания и обеспечения работы локальных реестров распределенного реестра создаются аппаратно-программные средства – узлы локальных реестров, которые можно рассматривать как рабочие места администраторов локальных реестров [2; 3]. На узлах создаются блоки данных для записи в реестр.

Все узлы работают в составе локальной сети учреждения либо региональной или местной сети.

Сеть должна обеспечивать возможность реализации установленных прав доступа к узлам для сотрудников учреждения, обеспечить защиту от несанкционированного доступа к реестрам, защиту каналов связи, обеспечить локализацию распределенного реестра в пределах учреждения. Существуют разнообразные решения данных задач, подробно исследованные в литературе [8; 14; 15].

Математические модели узлов локальных реестров

Создание распределенного реестра требует решения ряда задач и анализа, позволяющих получать численные значения характеристик работы распределенного реестра в зависимости от параметров (интенсивность потока запросов к реестру, интенсивность потока документов для занесения в реестр, длительность обработки запросов в реестре, структура и состав блоков реестра):

• анализ процессов формирования блоков документов на узлах для записи в локальные реестры;

• анализ процессов записи блоков в блокчейны локальных реестров и создания копий;

• анализ процессов обработки запросов пользователей реестра.

Для проведения анализа разработаны математические модели с поглощением сообщений, представленные в работах [13; 16–18]. Ряд моделей, позволяющих исследовать сетевые структуры, представлен в работе [14].

В данном случае поглощение элементарных сообщений (документов) подразумевает формирование из них блоков для записи в реестр.

В моделях каждый документ соответствует элементарному сообщению, а процесс формирования блока документов соответствует созданию сложного сообщения (блока) в системах с поглощением элементарных сообщений.

Как правило, число документов, поступающих для обработки и хранения конечно, поэтому в качестве модели узла рассматривалась система с фиксированным составом сложного сообщения (блока документов) и с ограниченным числом мест для ожидания в очереди элементарными сообщениями (документами).

При создании моделей считалось, что на узел поступает N потоков документов – элементарных сообщений ($\infty > N \geq 1$), из этих сообщений формируется **M** блоков (сложных сообщений). Правила формирования блоков на узлах задаются матрицей $\mathbf{M} = \|m_{ij}\|$, где $m_{ij} \geq 0$ – число документов потока номер j, которые входят в состав блока типа i (i = 1, 2,…, M; j = 1, 2,…, N) [19].

При формировании элементов матрицы **M** предполагалось соблюдение условий:

а) документы каждого потока могут участвовать при создании блоков только одного типа (для каждого сотрудника установлены наборы доступных документов и каждое подразделение создает свои блоки и документы);

б) в каждый блок входит хотя бы один документ.

Возможны варианты, учитываемые в математических моделях:

– длительность формирования блока не ограничена, и формирование заканчивается при поступлении необходимого количества документов;

– длительность формирования блока ограничена;

– число документов в блоке случайная величина.

Потеря документов в реестре исключается за счет задания на узлах достаточно большого количества мест для ожидания документами формирования блоков, в состав которых они войдут.

Модели для анализа вариантов представлены в работах [13; 16–18; 20]. Модели дают возможность дополнительно исследовать следующие варианты состава формируемых блоков документов: блок формируется из документов только одного типа (потока), количество которых задано; блок формируется из документов различных потоков, количество документов каждого потока задано.

Применение математических моделей позволяет вычислять значения характеристик реестра, в числе которых:

• средняя длительность формирования блока документов для записи в реестр;

• среднее время ожидания документом записи в реестр;

• средняя длина очереди документов;

• среднее время записи блока в реестр (при вычислении этой характеристики учитывается отсутствие состязаний при записи в реестр (блокчейн), и запись происходит в установленном для узлов администраторов порядке).

Модели позволяют варьировать параметры реестра (моделей, соответственно) для поиска оптимальных или приемлемых по значениям характеристик решений. Среди этих параметров:

• состав блока;

• средняя длительность формирования блока;

• допустимая длина очереди документов;

• количество узлов администрирования для локального реестра.

Математические модели анализа систем возможно применять для анализа процессов создания и эксплуатации распределенного реестра, работающего без определения очередности права записи формируемых блоков (сложных сообщений).

ВЫВОДЫ

Технология распределенных реестров и технология блокчейн сегодня занимают важное место в решении задач защиты информации: обеспечение целостности, защита от изменений данных, управление доступом, согласование данных.

Большое разнообразие практических приложений, где используются данные, требует разработки и предварительного анализа методов создания блоков данных для хранения в реестре, структуры и алгоритмов работы узлов распределенного реестра. Для решения этих задач целесообразно использовать математическое моделирование.

Данные о возможном создании и исследовании распределенного реестра на базе блокчейн для аэропорта можно масштабировать для случая авиатранспортной системы, для региональных систем управления авиаперевозками.

СПИСОК ИСТОЧНИКОВ

1. Башир И. Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты / Пер. с англ. М. А. Райтмана. – М.: ДМК Пресс, 2019. – 538 с. ISBN 978-5-97060-624-7.

2. Горбунова М. В. Омётов А. Я., Комаров М. М., Беззатеев С. В. Обзор проблем внедрения технологии распределенного реестра // Информационно-управляющие системы. – 2020. – № 2 (105). – С. 10–19. DOI: 10.31799/1684-8853-2020-2-10-19.

3. Носиров З. А., Фомичев В. М. Анализ блокчейн-технологии: основы архитектуры, примеры использования, перспективы развития, проблемы и недостатки // Системы управления, связи и безопасности. – 2021. – № 2. – С. 37–75. DOI: 10.24412/2410-9916-2021-2-37-75.

4. Khan, N. FAST: A MapReduce Consensus for High Performance Blockchains. In: Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. New York, NY, USA: Association for Computing Machinery, 2018, pp. 1–6. DOI: 10.1145/3282278.3282279.

5. Sadeghi, M., Mahmoudi, A., Deng, X. Adopting distributed ledger technology for the sustainable construction industry: evaluating the barriers using Ordinal Priority Approach. Environmental Science and Pollution Research, 2022, Vol. 29 (7), pp. 10495–10520. DOI: 10.1007/s11356-021-16376-y.

6. Sherman, A. T., Javani, F., Zhang, H., Golaszewski, E. On the Origins and Variations of Blockchain Technologies. IEEE Security Privacy, 2019, 17 (1), pp. 72–77. DOI: 10.1109/MSEC.2019.2893730.

7. Рябко Б. Я., Фионов А. Н. Криптография в информационном мире. – М.: Горячая линия – Телеком, 2018. – 300 с. ISBN: 978–5–9912–0729–4.

8. Столлингс В. Криптография и защита сетей: принципы и практика / Пер. с англ. 2-е изд. – М.: Издательский дом «Вильямс», 2001. – 672 с. ISBN: 5–8459–0185–5.

9. Чмора А. Современная прикладная криптография. – М.: Гелиос АРВ, 2001. – 256 с. ISBN: 5–85438–037–4.

10. Haber, S., Stornetta, W. S. How To Time-Stamp a Digital Document. Journal of Criptology, 1991, Vol. 3, Iss. 2, pp. 99–111. DOI: 10.1007/bf00196791.

11. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016, 336 p. ISBN: 978-0-691-17169-2.

12. Арсеньев Б. П., Яковлев С. А. Интеграция распределенных баз данных. – СПб.: Изд-во «Лань», 2001. – 464 с. ISBN: 5–8114–0300–3.

13. Pankov, K. N., Saksonov, E. A. Using Probabilistic Methods in the Analysis of Information Security of Distributed Ledger Systems. In: 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia. Institute of Electrical and Electronics Engineers Inc., 2021. DOI: 10.1109/IEEECONF51389.2021.9416006.

14. Вишневский В. М. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003. – 512 с. ISBN: 5–94836–011–3.

15. Таненбаум Э., М. ван-Стеен. Распределенные системы. Принципы и парадигмы. – СПБ.: Питер, 2003. – 877 с. ISBN: 5–272–00053–6.

16. Далингер Я. М. Анализ потоков сложных сообщений в системах обработки информации // Вестник Тихоокеанского государственного университета. – 2015. – № 1 (36). – С. 59–64. EDN: TPTDKD.

17. Dalinger, Ya. M., Leokhin, Yu. L., Saksonov E. A. The Model of the Processing Node with the Data Absorption. Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, Belarus, 2018, pp. 193–197. DOI: 10.1109/SYNCHROINFO.2018.8457008.

18. Saksonov, E. A., Leokhin, Yu. L., Dalinger, Ya. M. The Model of the Processing Node with the Data Replication. Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, Belarus, 2018, pp. 564–568. DOI: 10.1109/SYNCHROINFO.2018.8457025.

19. Далингер Я. М. Анализ потоков данных в системах с поглощением сообщений // Информатика и системы управления. – 2012. – № 3. – С. 26–34. [Электронная версия журнала]: https://ics.togudv.ru/media/2012/N33_03_1.pdf. Доступ 23.08.2024.

20. Maull, R., Godsiff, Ph., Mulligan, C., Brown, A., Kewell, B. Distributed ledger technology: Applications and implications. FINRA, 2017, Vol. 26, Iss. 5, pp. 481–489. DOI: 10.1002/jsc.2148 [доступ для подписчиков]. ●

Информация об авторах:

***Розенберг Игорь Наумович** – доктор технических наук, профессор, член-корреспондент Российской академии наук, научный руководитель Российского университета транспорта, Москва, Россия, info@science-rut.ru.*

***Далингер Яков Михайлович** – кандидат технических наук, проректор Российского университета транспорта, Москва, Россия, iakovdalinger@gmail.com.*

Статья поступила в редакцию 16.08.2024, одобрена после рецензирования 16.09.2024, принята к публикации 25.09.2024.