УДК 004.942 DOI:10.26102/2310-6018/2020.29.2.001

Математическое и имитационное моделирование закрытого распределенного реестра с управляющим узлом

В.А. Евсин, С.Н. Широбокова, С.П. Воробьев, В.А. Евсина
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, Новочеркасск, Россия

Резюме: В данной статье представлено математическое и имитационное моделирование распределенного реестра с управляющим узлом на примере алгоритма консенсуса RAFT. Описан процесс взаимодействия отдельных узлов сети распределенного реестра, особое внимание уделено алгоритму проведения транзакций внутри данной сети. Ключевым аспектом данной статьи является разработка математической модели сети распределенного реестра как системы массового обслуживания с использованием теории очередей. Рассмотрены концептуальные модели как распределенного реестра в целом, так и модель информационного процесса доступа к кластеру нотариальных узлов. Проведено математическое моделирование сети распределенного реестра, а также информационного процесса получения доступа к управляющему узлу сети. Представлено пространство состояний в распределенном реестре с управляющим узлом. Сформировано описание инфинитезимальной матрицы для оценки вероятности переходов между состояниями в распределенном реестре, описаны вероятности переходов, а также интенсивности данных процессов. Описана характеристика законов распределения показателей в рассматриваемой системе. Другим важным аспектом данной статьи является имитационное моделирование процесса с целью выявления наиболее качественной комбинации параметров для достижения максимальной эффективности. Сформирован стек варьируемых показателей имитационной модели. Проведены тесты, на основании которых эмпирическим методом подобрана наиболее эффективная совокупность характеристик. Представлены итоги по проведению математического и имитационного моделирования распределенного реестра с управляющим узлом.

***Ключевые слова*:** распределенный реестр, DLT-система, алгоритм консенсуса, математическое моделирование, инфинитезимальная матрица, теория массового обслуживания, теория очередей, имитационное моделирование.

Для цитирования: В.А. Евсин, С.Н. Широбокова, С.П. Воробьев, В.А. Евсина Математическое и имитационное моделирование закрытого распределенного реестра с управляющим узлом. *Моделирование, оптимизация и информационные технологии.* 2020;8(2). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/05/EvsinSoavtors_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.001

Mathematical and simulation modeling of a closed distributed registry with a control node

V.A. Evsin, S.N. Shirobokova, S.P. Vorobyov, V.A. Evsina
Platov South-Russian State Polytechnic University (NPI), Novocherkassk, Russia

Abstract: This article presents mathematical and simulation modeling of a distributed registry with a control node on the example of the raft consensus algorithm. The process of interaction

between individual nodes of the distributed registry network is described, special attention is paid to the algorithm for conducting transactions within this network. The key aspect of this article is the development of a mathematical model of a distributed registry network as a Queuing system using queue theory. We consider the conceptual models of both the distributed registry as a whole and the model of the information process for accessing a cluster of notary nodes. Mathematical modeling of the distributed registry network, as well as the information process of obtaining access to the control node of the network. The state space is represented in a distributed registry with a control node. The description of an infinitesimal matrix for estimating the probability of transitions between States in a distributed registry is formed, the transition probabilities and the intensity of these processes are described. The characteristic of the laws of distribution of indicators in the system under consideration is described. Another important aspect of this article is the simulation of the process in order to identify the best combination of parameters to achieve maximum efficiency. A stack of variable indicators of the simulation model is formed. Tests were carried out on the basis of which the most effective set of characteristics was selected empirically. The results of mathematical and simulation modeling of a distributed registry with a control node are presented.

Keywords: distributed registry, DLT system, consensus algorithm, mathematical modeling, infinitesimal matrix, Queuing theory, queue theory, simulation modeling.

For citation: Evsin V.A., Shirobokova S.N., Vorobyov S.P., Evsina V.A. Mathematical and simulation modeling of a closed distributed registry with a control node. *Modeling, Optimization and Information Technology*. 2020;8(2). Available from: https://moit.vivt.ru/wp-content/uploads/2020/05/EvsinSoavtors_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.001 (In Russ).

Введение

Одним из наиболее актуальных методов организации хранения данных в настоящее время является реализация систем распределенного реестра. Такие системы позволяют сформировать защищенную систему, в которой все данные находятся в согласованном состоянии на основании алгоритма консенсуса [1-3]. Распространенной вариацией алгоритма консенсуса является алгоритм *RAFT,* основанный на одноименном архитектурном решении, модифицированный с учетом работы в установившемся режиме в пределах одного срока действия лидирующего узла. Лидирующий узел в данном алгоритме консенсуса, называемый нотариальным узлом, верифицирует и подписывает транзакции. Проблемой при реализации распределенных реестров является неэффективное планирование топологии и состава комплектующих элементов, которое приводит к снижению качества работы сети, что может быть критично для систем, требующих высокой отказоустойчивости. Для решения поставленной проблемы может быть использовано математическое моделирование с использованием теории массового обслуживания для распределенного реестра.

Информационные процессы в распределенном реестре

Общая система распределенного реестра рассматриваемого типа представляет собой *peer-to-peer* сеть, в которой канал связи защищен протоколами *X.509.*

Для реализации согласованных состояний каждый объект должен формировать модель состояний. Каждое новое состояние объекта обновляется у всех участников транзакции, при этом все предыдущие состояния данного объекта невозможно использовать в будущих транзакциях. Этот процесс решает проблему двойного расходования, что наиболее эффективно проявляет себя в финансовых операциях [4,5]. При реализации

каждой транзакции формируется поток на обновление состояний объектов распределенного реестра. В ходе обновления состояния объектов для каждого нового объекта формируется цепочка хеш-функций для согласования и защиты последовательности транзакций с объектами. Хеш-функция рассчитывается с использованием алгоритма дерева Меркла. Каждая последующая транзакция учитывает хеш-функции предыдущих, что позволяет верифицировать транзакции с учетом всех предыдущих состояний объектов. Таким образом производится обмен информационными ресурсами.

Математическая и имитационная модель распределенного реестра

На концептуальном уровне закрытый распределенный реестр с управляющим узлом представляет собой систему массового обслуживания, для описания которой может быть использована теория очередей. Концептуальная модель распределенного реестра как системы массового обслуживания [6-8] представлена на Рисунке 1.

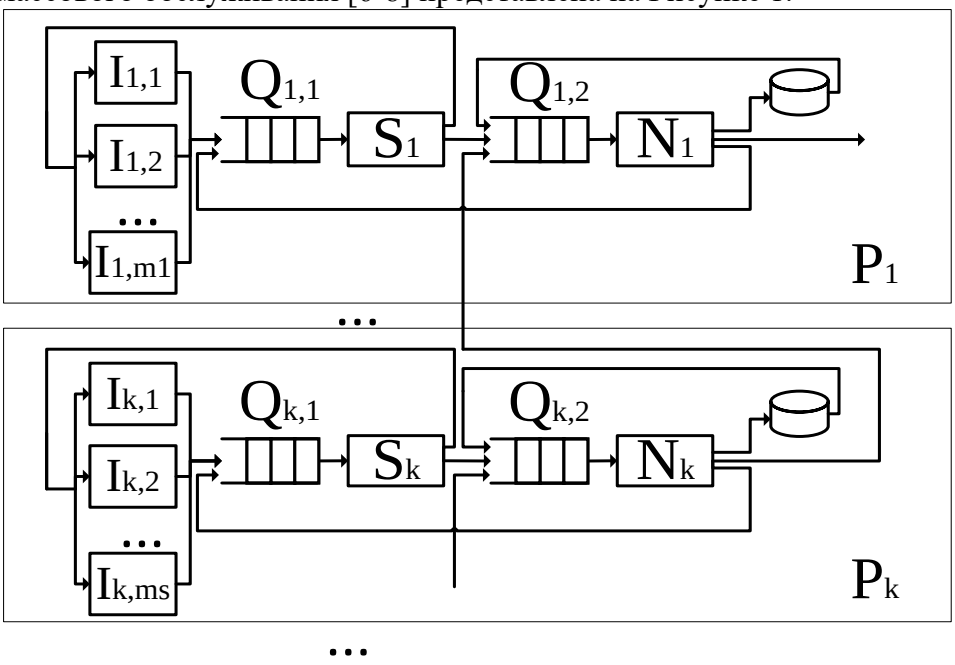

Рисунок 1 – Модель взаимодействия узлов в сети распределенного реестра
Figure 1 – Model for interaction of nodes in a distributed registry network

На представленном Рисунке $I_{k,s}-$ клиентские приложения, $Q_{k,1}-$ очередь перед сервером, $Q_{k,2}-$ очередь перед узлом, P_k- участник сети распределенного реестра, S_k- сервер, N_k- узел сети распределенного реестра, для представленных индексов действуют следующие ограничения $k=\overline{1,K^s}$, $s=\overline{1,m_k}$. Для отдельного участника состояние сети представляет собой вектор (i_1,i_2), где i_1- количество заявок, находящихся в очереди и на обработке сервером, i_2- количество заявок в очереди и на обработке узлом сети. Динамическая система задается полным пространством состояний, который для данной модели сети имеет вид: $i_1=\overline{0,m_1}, i_2=\overline{0,m_2}$. При этом общее количество заявок на сервере и на узле не может быть больше, чем общее количество клиентских приложений для данного узла сети, т.е. $i_1+i_2\le m_1$. Исходя из данного контекста, элементы инфинитезимальной матрицы [9,10] имеют вид: $Q=\left\|q_{i1,i2,j1,j2}\right\|$, данные элементы представляют собой интенсивности перехода из состояния (i_1,i_2) в состояние (j_1,j_2) за бесконечно малый промежуток Δt. Диагональные элементы

матрицы Q равны сумме элементов строки, взятых со знаком «минус». Элементы инфинитезимальной матрицы представлены в Таблице 1.

Таблица 1 – Элементы формирования инфинитезимальной матрицы
Table 1 – Elements of forming an infinitesimal matrix

Событие и качественное описание условия	Формальное представление	Интенсивность переходов
1. Формирование заявки	$j_1 = i_1 + 1$; $j_2 = i_2$;	$(m - i_1 - i_2) * \lambda_1$
2. Окончание обработки заявки на сервере, после чего заявка отправляется клиентской части	$j_1 = i_1 - 1$; $j_2 = i_2$;	$p_{11} * \mu_1$
3. Окончание обработки заявки на сервере, после чего заявка отправляется на узел	$j_1 = i_1 - 1$; $j_2 = i_2 + 1$;	$p_{12} * \mu_1$
4. Получение заявки от другого узла сети	$j_1 = i_1$; $j_2 = i_2 + 1$;	λ_2
5. Окончание обработки заявки на узле, после чего заявка отправляется на сервер	$j_1 = i_1 + 1$; $j_2 = i_2 - 1$;	μ_2
6. Окончание обработки заявки на узле, после чего заявка обращается к БД	$j_1 = i_1$; $j_2 = i_2 - 1$;	$p_{22} * \mu_2$
7. Окончание обработки заявки на узле, после чего заявка отправляется к i-му узлу сети	$j_1 = i_1$; $j_2 = i_2 - 1$;	$p_{2i} * \mu_2$
8. Пребывание сети в текущем состоянии	$j_1 = i_1$; $j_2 = i_2$;	$-\sum_{i1 i2 j1 j2} q_{i1 i2 j1 j2}$
9. Прочие условия		0

В представленной Таблице вероятность отправки заявки на клиентское приложение или на узел распределенного реестра – p_{1i}; вероятность того, что заявка попадет на сервер или i-й узел сети распределенного реестра. Из закона сложения вероятностей следует $\sum_i p_{1i} = \sum_i p_{2i} = 1$. Данная математическая модель в достаточной степени описывает информационные процессы, протекающие в распределенном реестре, однако, ввиду большой размерности пространства состояний нецелесообразно определять вероятностные характеристики теории массового обслуживания на основе математической модели. Менее энергозатратной процедурой является разработка имитационной модели, которая разработана с учетом особенностей концептуальной модели распределенного реестра.

При проведении имитационного моделирования предполагается, что основные характеристические показатели распределены по закону Пуассона. Задача имитационного моделирования состоит в определении параметров, при которых работа сети будет максимально эффективной, что подразумевает среднюю нагрузку на узлы не менее 50%, при этом не более 75%. Данные параметры в наиболее полной форме характеризуют эффективную работу сервера.

Была произведена серия экспериментов, условия эксперимента с набором параметров, которые дали наиболее эффективный результат работы сервера, представлены в Таблице 2.

Таблица 2 – Условия эксперимента по определению наиболее качественного набора компонент распределенного реестра
Table 2 – Experimental conditions for determining the best quality set of distributed registry components

Наименование условия эксперимента	Величина
1. Количество участников сети	30
2. Количество клиентов для рассматриваемой СМО	45
3. Максимальный размер очереди перед сервером	25
4. Средняя длительность активного состояния, с	30
5. Вероятность отправки заявки на клиент из сервера	0,25
6. Вероятность отправки заявки на сервер из ноды	0,43
7. Вероятность отправки заявки на i+1 – ю ноду из текущей ноды	0,27
8. Размер очереди на ноде	20
9. Время обработки заявки на сервере, с	20
10. Время обработки заявки на ноде, с	7
11. Время выполнения эксперимента, с	1000

Результаты эксперименты представлены в Таблице 3.

Таблица 3 – Результаты эксперимента по определению наиболее качественного набора компонент распределенного реестра
Table 3 – Results of an experiment to determine the best quality set of distributed registry components

Наименование результата эксперимента	Величина
1. Средняя загруженность очереди перед сервером, с	0,742
2. Общее время максимальной загруженности очереди сервера, с	358
3. СКО загруженности очереди перед сервером	0,643
4. Вероятность нахождения очереди перед сервером в состоянии максимальной загруженности	0,25
5. Средняя загруженность очереди перед нодой	0,72
6. Общее время максимальной загруженности очереди перед нодой, с	0
7. СКО загруженности очереди перед нодой	0,825
8. Вероятность нахождения очереди перед нодой в состоянии максимальной загруженности	0

Следовательно, при заданном наборе входных параметров эксперимент признан удачным, средняя загруженность очереди перед узлом сети составила 72%, что является удовлетворительным результатом.

Математическая и имитационная модель кластера управляющих узлов

Верификация транзакции реализуется кластером нотариальных узлов, которые производят проверку всех входных данных транзакции с целью выявления отклонений. Кластер нотариальных узлов в терминах архитектурного решения *RAFT* представлен управляющими узлами, которые, однако, не меняются со временем, но управляют

маршрутизацией и реализуют контроль над транзакциями в сети распределенного реестра. Математическая модель информационного процесса при проведении верификации транзакций может быть описана с использованием теории массового обслуживания. Концептуальная модель кластера управляющих узлов представлена на Рисунке 2.

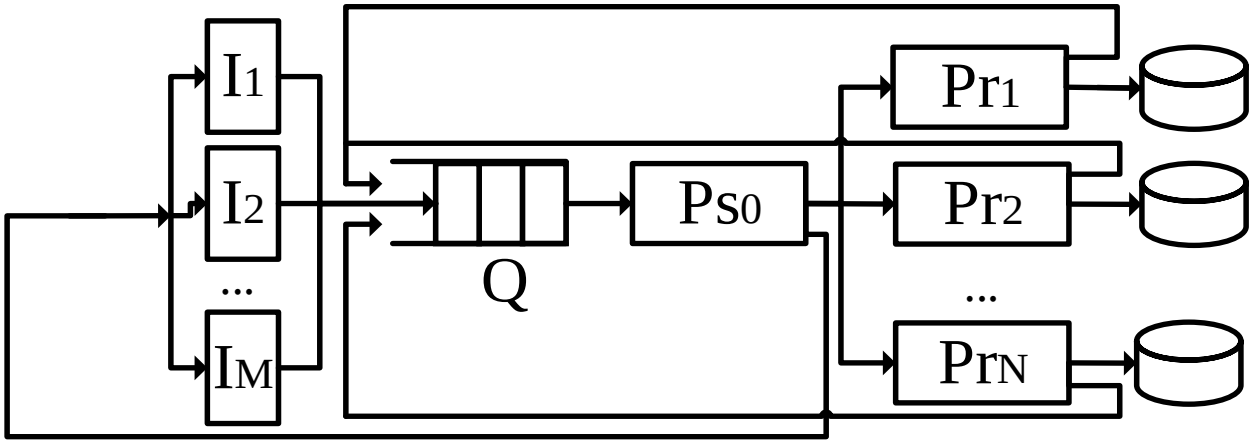

Рисунок 2 – Концептуальная модель кластера управляющих узлов
Figure 2 – Conceptual model of a cluster of control nodes

На данном Рисунке представлена сеть, которая обрабатывает запросы и состоит из узлов-клиентов $(I_1, I_2, \dots, I_M)$, сервера распределения Ps_0 и кластера узлов-нотариусов $(Pr_1, Pr_2, \dots, Pr_N)$.

Для каждого отдельного участника состояние сети задается вектором (i, j, k), где i – количество заявок, находящихся в очереди, j – количество свободных обработчиков заявок, k – количество работоспособных обработчиков заявок. Полное пространство состояний для данной модели сети имеет вид: $i = \overline{0, M}, j = \overline{0, N}, k = \overline{0, N}, M$ – количество клиентских узлов, N – количество узлов нотариусов в кластере. Элементы инфинитезимальной матрицы $Q = \|q_{i.j.k}\|$ представляют собой интенсивности перехода из состояния (i_1, j_1, k_1) в состояние (i_2, j_2, k_2) за бесконечно малый промежуток времени Δt.

Ввиду большой размерности данной математической модели целесообразно провести имитационное моделирование информационного процесса получения доступа к кластеру управляющих узлов. Задача имитационного моделирования состоит в определении оптимального количества узлов-нотариусов. В результате проведения серии экспериментов были определены наиболее оптимальные параметры. Условия проведения оптимального эксперимента представлены в Таблице 4.

Таблица 4 – Условия эксперимента по определению наиболее качественного набора компонент распределенного реестра
Table 4 – Experimental conditions for determining the best quality set of distributed registry components

Наименование условия эксперимента	Величина
1. Количество источников заявок	600
2. Тип запроса	Однократный
3. Дисциплина обслуживания	*FIFO*
4. Среднее время активного состояния участника, с	300

5. Очередь перед сервером распределения	400
6. Среднее время распределения заявок, с	10
7. Среднее время обработки заявок, с	70

В результате выполнения эксперимента был получен результат по средней загруженности очереди, равный 82%, при этом вероятность того, что очередь будет загружена в произвольный момент – 57%, что можно назвать удовлетворительным результатом. Таким образом проведено моделирование доступа к управляющим узлам.

Заключение

По результатам проведенных исследований представлена математическая модель распределенного реестра с управляющим нотариальным узлом, а также сформирована имитационная модель, на основании которых определены наиболее оптимальные параметры для заданных условий топологии распределенного реестра. Сформированы концептуальные модели распределенных реестров как систем массового обслуживания, на основании данных моделей определены элементы инфинитезимальной матрицы, а также имитационные модели распределенного реестра.
Данные модели могут быть использованы для повышения качества работы сети распределенного реестра с управляющим кластером узлов.

ЛИТЕРАТУРА

1. Тапскотт Д. *Технология блокчейн: то, что движет финансовой революцией сегодня*. М.: Эксмо. 2017:448.
2. Евсин В. А., Широбокова С. Н., Продан Е. А. Использование технологии распределенных реестров при проектировании информационной системы «Аренда недвижимости» с применением искусственных нейронных сетей. *Инженерный вестник Дона*. 2018;1. Доступно по: ivdon.ru/ru/magazine/archive/n1y2018/4655.
3. Савельев А. И. Договорное право 2.0: "Умные" контракты как начало конца классического договорного права. *Вестник гражданского права*. 2016;3:32-60.
4. Андрюшин С. А. Технология распределенных реестров в финансовой сфере России. *Банковское дело*. 2018;2:4-15.
5. Нараевский О. А., Евсин В. А. Формализованный анализ функциональной полноты платформ распределённых реестров. *Фундаментальные основы, теория, методы и средства измерений, контроля и диагностики*: матер. 19-ой Междунар. молодежной науч.-практ. конф. (г. Новочеркасск, 27-28 фев. 2018). 2018:396-404.
6. Хемди А. Таха. *Введение в исследование операций*. М.: Вильямс. 2005:912.
7. Климов Г. П. *Теория массового обслуживания*. М.: МГУ. 2011:312.
8. Халин В. Г. *Теория принятия решений. Учебник и практикум*. М.: Юрайт. 2017;2:432.
9. Черноморов Г. А. *Теория принятия решений*: Учебное пособие. Новочеркасск: Ред. журн. «Изв. Вузов. Электромеханика», 2005:448.
10. Chakka R., Harrison P. G. A Markov modulated multi-server queue with negative customers –Ihe MM CPP/GE/c/LG-queue. *Acta Informatika*. 2001;37:785-799.

REFERENCES

1. Tapscott D. *Blockchain Technology: what drives the financial revolution today*. Moscow: Eksmo. 2017: 448.
2. Evsin V. A., Shirobokova S. N., Prodan E. A. Use of distributed registry technology in the design of the information system "real estate rental" using artificial neural networks. *Engineering Bulletin of the don*. 2018;1. Available by: ivdon.ru/ru/magazine/archive/n1y2018/4655.
3. Savelev A. I. Contract law 2.0: Smart contracts as the beginning of the end of classical contract law. *Bulletin of civil law*. 2016;3:32-60.
4. Andryushin S. A. Technology of distributed registers in the financial sphere of Russia. *Banking*. 2018;2:4-15.
5. Narayevsky O. A., Evsin V. A. Formalized analysis of the functional completeness of distributed registry platforms. *Fundamentals, theory, methods and tools of measurement, control and diagnostics*: materials of the 19th international conference. youth scientific and practical Conf. (Novocherkassk, Feb. 27-28, 2018). 2018:396-404.
6. Hemdi A. Taha. *Introduction to operations research*. Moscow: Williams. 2005:912.
7. Klimov G. P. *Theory of Queuing*. Moscow: MSU. 2011:312.
8. Khalin V. G. *Theory of decision-making*. The tutorial and workshop. Moscow: Yurayt. 2017;2:432.
9. Chernomorov G. A. *Theory of decision-making*: Textbook. Novocherkassk: Ed.-«WPI. Higher educational. Elektromekhanika", 2005:448.
10. Chakka R., Harrison P. G. A Markov modulated multi-server queue with negative customers –Ihe MM CPP/GE/c/LG-queue. *Acta Informatika*. 2001;37:785-799.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Евсин Владимир Александрович, аспирант, кафедра “Информационные и измерительные системы и технологии”, Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, Новочеркасск, Российская Федерация
email: ewsin.wladimir95@gmail.com

Vladimir A. Evsin, postgraduate student, Department "Information and measuring systems and technologies", Platov South-Russian State Polytechnic University (NPI), Novocherkassk, Russian Federation

Широбокова Светлана Николаевна, доцент, к.э.н., доцент кафедры “Информационные и измерительные системы и технологии”, Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, Новочеркасск, Российская Федерация
email: shirobokova_sn@mail.ru

Svetlana N. Shirobokova, associate Professor, Candidate of Economic Sciences, associate Professor, Department "Information and measuring systems and technologies", Platov South-Russian State Polytechnic University (NPI), Novocherkassk, Russian Federation

Воробьев Сергей Петрович, доцент, к.т.н., доцент кафедры “Информационные и измерительные системы и технологии”, Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, Новочеркасск, Российская Федерация
email: vsp1999@yandex.ru

Sergei P. Vorobyev associate Professor, Candidate of Engineering Sciences, associate Professor, Department "Information and measuring systems and technologies", Platov South-Russian State Polytechnic University (NPI), Novocherkassk, Russian Federation

Евсина Виктория Александровна, студент, 3 курс, кафедра “Прикладная математика”, Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, Новочеркасск, Российская Федерация
email: Viktoryews1997@mail.ru

Viktorya A. Evsina, student, 3 course, Department “Applied Mathematics”, Platov South-Russian State Polytechnic University (NPI), Novocherkassk, Russian Federation