УДК 004.75 DOI:10.31854/1813-324X-2021-7-1-122-131

Научные аспекты структурно-параметрического моделирования блокчейн-систем

А.В. Спиркина[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: spirkina.av@gmail.com

Информация о статье
Поступила в редакцию 10.02.2021
Принята к публикации 15.03.2021

Ссылка для цитирования: Спиркина А.В. Научные аспекты структурно-параметрического моделирования блокчейн-систем // Труды учебных заведений связи. 2021. Т. 7. № 1. С. 122–131. DOI:10.31854/1813-324X-2021-7-1-122-131

Аннотация: *В течение последнего десятилетия помимо мультисервисных сетей существенное развитие получила технология блокчейн из-за возможности организации безопасного, целостного, надежного обмена и хранения информации. В силу большой востребованности технологии возникает проблема передачи данных на сети операторов связи. При этом появляется ключевая задача рассмотреть влияние данной технологии на сетевые характеристики для прогнозирования поведения трафика на сети и обеспечения требуемых показателей качества услуг, а также стабильности состояния элементов сети связи общего пользования при работе технологии распределенного реестра. Однако рассмотреть и проанализировать влияние технологии в натурном эксперименте является трудозатратной задачей, которая не всегда может быть выполнена, поэтому в данной статье предлагается рассмотреть подходы к структурно-параметрическому моделированию данных систем.*

Ключевые слова: *блокчейн, распределенный реестр, децентрализованные системы, имитационное моделирование, аналитическое моделирование.*

Введение

В настоящее время сети связи являются основой для создания системы, направленной на поддержку цифровизации мирового сообщества, поэтому необходимо обеспечить не только их устойчивое функционирование в настоящий момент, но и обратить внимание на перспективы развития [1]. Предполагается, что критерии безопасности, конфиденциальности, надежности, высокой скорости передачи данных для таких систем будут являться ключевыми, и им должно быть уделено особое внимание со стороны исследовательского сообщества.

Для решения вышеупомянутых проблем можно применять перспективную технологию блокчейн, которая позволит создавать новые формы распределенных архитектур, при этом использоваться для определения всей технологической системы, стоящей за обменом цифровыми активами между участниками одной сети без посредников [2, 3].

Блокчейн – это распределенная база данных, состоящая из постоянно обновляемого списка структурированных данных, у которой устройства хранения и обработки данных не подключены к общему серверу [4, 5]. Основными преимуществами блокчейн-технологии [3–5] можно считать децентрализацию, надежность системы, так как при любой попытке внесения несанкционированных изменений транзакция будет отклонена из-за несоответствия предыдущим копиям и проверки добавленных данных независимыми участниками.

Сегодня исследователи, разработчики предполагают, что технология блокчейн, хоть и является новой и неоднозначной, может изменить часть современных услуг. Возможности блокчейна делают его применение привлекательным для компаний, работающих в разных областях, основные кандидаты на внедрение блокчейна – финансовая сфера, телекоммуникационная область, транспорт, промышленность и агропромышленный комплекс. В отчете американской аналитической компании Transparency Market Research указано, что мировой рынок блокчейна к 2024 г. составит 20 млрд. долларов, а рост индустрии составит около 59 % в год. В компании Grand View Research было проведено аналогичное исследование. При этом GVR прогнозирует объем индустрии на уровне 7,74 млрд. долларов к 2024 г. [6].

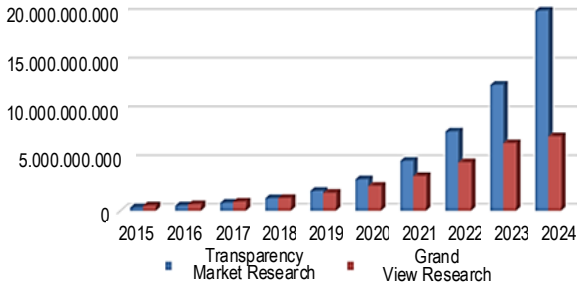

Рис. 1. Динамика роста рынка блокчейн [6]

Fig. 1. Growth Dynamics of the Blockchain Market [6]

Несмотря на значительную разницу в конечных цифрах, по мнению многих исследователей, рынок будет быстро расти и развиваться, что подчеркивает потребности существующих систем в интеграции. Блокчейн позволит создать новые формы взаимодействия, где участники сети будут использовать для транзакционного обмена данных через большую сеть недоверенных участников, не полагаясь на центральный узел [2]. При этом нельзя не обратить внимания на то, что данная технология может существенным образом отразиться на сфере телекоммуникаций.

Технология предполагает задействовать большое число узлов на сети для решения задач с дополнительным объемом служебного трафика и постоянным обменом данными. Таким образом, появляется необходимость рассмотреть ее влияние на сеть и определить вопросы проработки текущей сетевой инфраструктуры под новые требования, так как на этапе фактического развертывания может проявиться негативное влияние [5–7]. На сегодняшний день все еще не хватает унифицированных инструментов для оценки показателей при работе блокчейн-технологии, однако количество используемых блокчейн-приложений уже достигло высоких количественных показателей [8].

Технические аспекты блокчейн-технологии

В развитии блокчейна можно выделить два основных поколения. Первое поколение – это открытая бухгалтерская книга для денежных транзакций с ограниченными возможностями поддержки программируемых транзакций. Типичным примером являются приложения для обмена криптовалютой. Второе поколение блокчейнов стало общепрограммируемой инфраструктурой с общедоступным реестром, в котором записываются результаты вычислений, примером являются интеллектуальные контракты, голосование и цепочки поставок [2].

Технология блокчейна представляет собой специализированную информационно-коммуникационную технологию с некоторыми характерными особенностями. Ключевыми объектами системы, определяющими новые возможности, являются узлы, транзакции и алгоритмы консенсусов.

Транзакция – это подписанная структура данных, выражающая передаваемое значение. Транзакции представляют собой переходы состояний с информацией о владельце (сообщение), которые могут включать новые записи данных и передачу между участниками. Каждая транзакция состоит из входного и выходного раздела, а также – цифровой подписи.

Блоки – это контейнеры, агрегирующие транзакции для дальнейшего включения в публичный реестр. Каждый блок является идентифицируемым и связан с его предыдущим блоком в цепочке. Он состоит из заголовка, содержащего метаданные, и тела из списка транзакций.

Узел – это устройство на блокчейн-сети, позволяющее ей функционировать. Это может быть любое активное электронное устройство, подключенное к сети Интернет. В зависимости от функциональности существуют различные типы узлов:

– полные узлы реализуют полный протокол блокчейна и содержат полную копию реестра; их технические возможности подразумевают обнаружение и общение с другими узлами, отправку, получение и хранение блоков, проверку транзакций; полный узел может автономно проверять транзакции, при этом храня большой объем данных, и проводить синхронизацию для обновления актуальных данных;

– легкие узлы не хранят закрытые ключи и не подписывают транзакции сами; такой узел хранит только заголовок каждого блока в своем локальном хранилище; преимущество легких клиентов перед другими типами клиентов заключается в том, что пользователю не нужно постоянно синхронизировать весь реестр, что подразумевает минимальные технические требования.

Майнеры – клиенты, которые используются для подтверждения транзакций и поиска решения головоломки с целью получения прибыли.

Также в большинстве блокчейн-систем представлены и другие виды узлов, например, узлы отслеживания (суперузлы), скоростные узлы и другие. Однако все узлы должны включать функции маршрутизации для проверки/распространения сообщений и обслуживания соединений. Алгоритм работы блокчейн-технологии для узлов, участвующих в эксперименте, представлен на рисунке 2 [7].

Работу блокчейн-технологии можно разделить на несколько этапов (обнаружение сети, создание транзакции и ее проверка, майнинг, проверка блока на корректность).

Этап 1. Обнаружение сети. При первом подключении узла к сети происходит его загрузка, а также соединение с узлом начальной загрузки для получения списка соседних узлов, синхронизации и получения актуальной версии цепочки блоков, в дальнейшем происходит отключение.

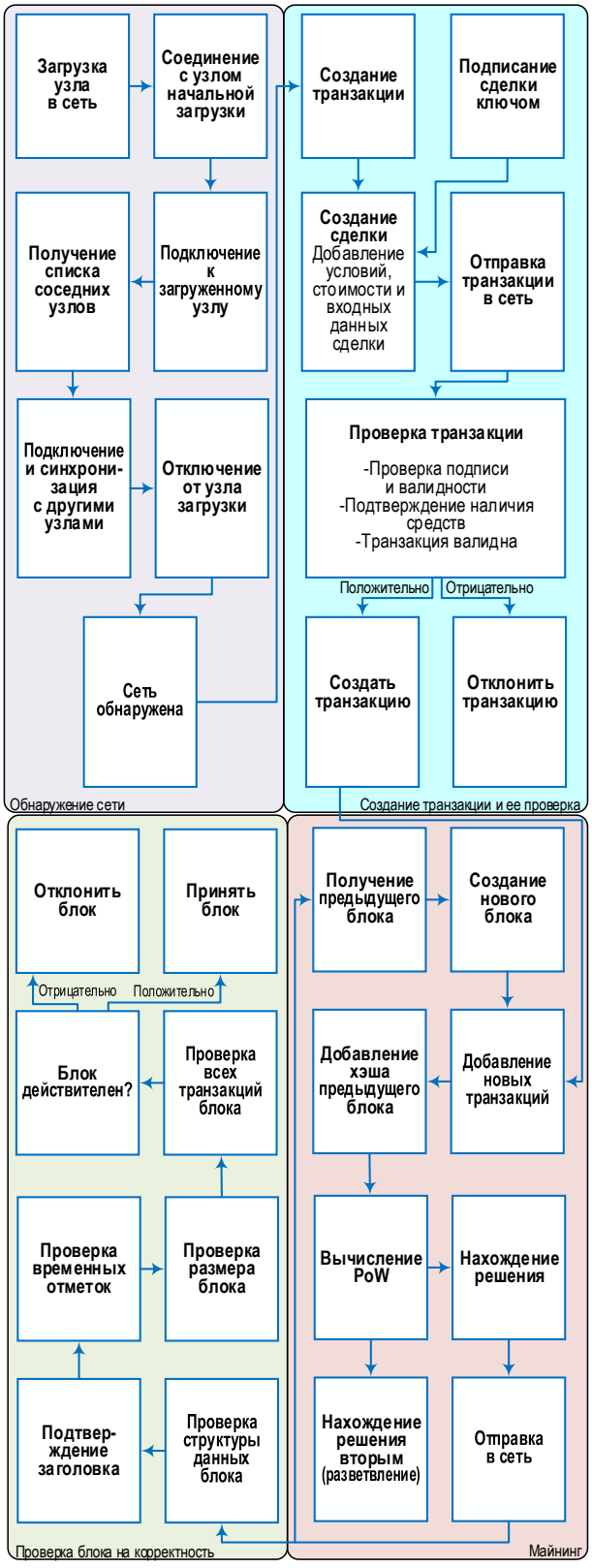

Рис. 2. Алгоритм работы блокчейн-технологии [7]

Fig. 2. Algorithm of Blockchain Technology [7]

Этап 2. Создание транзакций и проверка. Создание новой транзакции подразумевает выполнение некоторых условий участниками обмена, поэтому в транзакции прописываются сумма и адресат, а также дополнительно могут быть обозначены условия выполнения сделки. После создания транзакции отправитель подписывает ее своим электронным ключом и отправляет в сеть. При этом транзакция будет отклонена, если она сформирована неправильно, недействительна или не содержит всю информацию, необходимую для выполнения, также транзакция будет отклонена, если у пользователя недостаточно средств для выполнения операции.

Этап 3. Майнинг. После получения новой транзакции узел инициализирует ее добавление в блок. Блок формируется на основании информации о прошлом принятом блоке и информации собранной на данном этапе. Майнеры пытаются найти решение, блок проверяется, добавляется в реестр и направляется в сеть другим узлам. В случае, если решение было найдено вторым, то оно отбрасывается, чтобы избежать ветвления.

Этап 4. Проверка блока на корректность. Проверка блока перед добавлением в реестр подразумевает, что предыдущий блок существует, структура данных не нарушена, что у отправителя достаточно средств, что подпись верна, синтаксис корректен, входы и выходы в пределах допустимого значения, размер транзакции не выше максимального, что транзакция еще не была обработана. В случае подтверждения происходит обновление цепочки в общем реестре, происходит валидация транзакции и статуса пользователя. При отсутствии ошибок каждый узел обрабатывает и записывает «блок» в свою базу данных. Происходит завершение транзакции. После попадания в блокчейн и подтверждения достаточным количеством последующих блоков, транзакция становится неотъемлемой частью реестра и признается действительной всеми участниками.

Развитие новой технологии и ее популяризация вносят существенные изменения в форму сетевого взаимодействия между устройствами. Как уже упоминалось в [9], в процессе обмена блокчейн генерирует дополнительный трафик для обновления реестров на всех задействованных узлах, и увеличенного объема служебного трафика, который появляется при шифровании данных и заметно снижает долю полезного трафика. Предварительные расчеты и моделирование помогут подготовить сеть к работе с необходимым количеством устройств и рассчитать ключевые параметры и возможности взаимодействия.

Анализ систем моделирования блокчейн

Сегодня симуляция и аналитическое моделирование являются стандартными инструментами для оценки поведения и производительности большинства решений на основе блокчейнов [10].

Моделирование применяется в случае, если проведение экспериментов с реальными объек-

тами/системами неудобно, невозможно или слишком затратно. Главное отличие моделирования от других методов изучения сложных систем – возможность оптимизации системы до ее реализации. Поскольку много приложений, реализующих блокчейн, сложны в развертывании на тестовых сетях, моделирование и симуляция систем является важным аспектом для оценки производительности.

Традиционно модели разделяют на аналитические и имитационные. Аналитическая модель создается на основе теории или гипотезы, описывает определенный аспект системы с помощью математических выражений, и позволяет получать конечные результаты исследования в виде формальных соотношений, пригодных для количественного и качественного анализа. Данный тип моделей обычно применяют для описания фундаментальных свойств объектов.

На сегодняшний день в области решений блокчейн моделирование сетевых процессов развито слабо. Однако исследователи уже пытаются определить математические модели для описания процессов работы блокчейн-технологии и их зависимостей. Так, в таблице 1 приведено сравнение наиболее значимых решений в области аналитического моделирования.

Имитационные модели создаются с помощью стандартных программных средств с использованием стандартных вычислительных систем. Неоспоримым достоинством имитационного моделирования является возможность получения численных решений для тех моделей, которые не могут быть описаны конечными аналитическими выражениями [20]. Разумеется, не все задачи могут быть решены с использованием имитационного моделирования, например, задачи, требующие слишком большого объема вычислений из-за ограниченного ресурса вычислительных систем и конечного времени выполнения операций.

Для обеспечения качества предоставляемых услуг и стабильности состояния элементов сети связи при использовании технологии распределенных реестров планируется обеспечить за счет разработки эффективных моделей и методов прогнозирования трафика.

В настоящий момент существует несколько решений для моделирования работы блокчейн-технологии на сети связи, которые позволяют проводить различные проверки перед принятием окончательного решения о внедрении. В таблице 2 приведено сравнение наиболее значимых решений в области симуляции.

Моделирование блокчейн-систем на сети связи

Так как современные сети предоставляют широкий спектр услуг, то передача каждого вида трафика требует соблюдения некоторых условий к ряду параметров качества обслуживания, таких как задержка, потери, джиттер и другие. В связи с чем появляется необходимость моделирования систем и оценки параметров, поскольку при появлении трафика новых приложений существующие модели и характеристики трафика изменяются. В дальнейшем предлагается рассмотреть моделирование разных участков системы при передаче пользовательского трафика.

В настоящее время трафик пользовательских сессий относят к пуассоновским моделям [21], но при передаче гетерогенного трафика возможно наблюдать проявление самоподобия, которое оценивается коэффициентом Херста. Преобладание непуассоновского трафика приводит к необходимости использования моделей $G/G/v$, $G/D/v$ для описания аналитических методов [22, 23].

В предлагаемой системе для описания характера потоков данных сторонних приложений на уровне доступа рассмотрим модели с интервалами времени между заявками пакетов, формируемых по простейшему закону распределения, широко применяемого при анализе и проектировании сетей передачи данных (M_{NET}). Интервал времени между заявками приложений блокчейн, согласно представленным в таблице 1 решениям, отнесем к Марковскому (M_{BC}). Согласно свойствам таких потоков, на маршрутизаторе суммарный поток (M_{NET+BC}) сходится к простейшему потоку с интенсивностью, равной сумме интенсивностей исходных потоков [24].

При этом закон распределения времени обслуживания такого трафика будет описан зависимостями с преобладанием самоподобия, которое возникает в результате объединения множества изолированных источников [25]. Для моделирования самоподобного потока используют различные ONOF-методы, которые подразумевают формирование интересующего потока путем объединения потоков от нескольких источников [26]. Таким образом, из-за свойств пульсирующего трафика на оборудовании уровня агрегации распределение времени обслуживания трафика будет подчиняться закону с «тяжелыми хвостами» (Парето, Вейбулла и логнормальное распределения и др.). Рассмотрим распределение Парето для времени обслуживания трафика как наиболее подходящее по характеристикам [27]. Следовательно, упрощенную модель системы можно рассмотреть как $M_{NET+BC}/P_a/v$, а при рассмотрении и оценке характеристик каждого устройства – $M_{NET+BC}/P_a/1$.

Функция распределения Парето определяется следующим образом:

$$F(t) = 1 - (\frac{M}{t})^a \text{ при } t \geq M, t > 0, M > 0, \qquad (1)$$

где M – параметр масштаба; A – параметр формы.

ТАБЛИЦА 1. Решения в области аналитического моделирования для блокчейн-систем

TABLE 1. Analytical Modeling Solutions for Blockchain Systems

Исследование	Представленное решение	Инструмент/ технология	Рассматриваемые параметры и моделируемые характеристики
[11]	Моделирование процесса, используя несколько очередей на основе четырех фаз (ожидание включения в блок; ожидание подтверждения; ожидание обслуживания; обслуживание).	Граф перехода состояний; Теория массового обслуживания; Марковские процессы	Моделирование генерации блока; Вероятности перехода состояний; Задержки доступа
[12]	Модель организации майнинга определяют $M/M/n/L$. Емкость очереди устанавливается как T_xB, политика очереди – First Come First Serve, а правило отбрасывания – Block After Service, что означает, что только транзакции размера блока T_xB остаются в динамической памяти узлов майнинга, в то время как другие транзакции, даже если они обрабатываются, находятся в пуле памяти.	Теория массового обслуживания	Среднее количество транзакций на блок; Общая мощность майнинга; Количество транзакций в секунду
[13]	Модель $M/M/1$ используется для моделирования пула памяти блокчейна, а майнинг пул моделируется моделью $M/M/n$. В любой момент времени в пуле майнинга может быть только один блок. Однако внутри пула майнинга процессы могут быть разделены на множество задач или потоков для параллельной обработки несколькими узлами майнинга в сети.	Теория массового обслуживания	Среднее количество транзакций на блок; Скорость поступления транзакций; Среднее время майнинга каждого блока; Пропускная способность системы/транзакций; Время ожидания в пуле памяти; Количество неподтвержденных транзакций во всей системе; Общее количество транзакций
[14]	Процесс майнинга моделируется с помощью системы очередей, анализируя время подтверждения транзакции. В решении представлена модель $M/G/1$ с пакетным обслуживанием, в котором вновь поступающая транзакция не может попасть в объект обслуживания, даже если количество транзакций в средстве обслуживания не достигает максимального размера пакета. В этой модели время пребывания транзакции соответствует времени ее подтверждения.	Теория массового обслуживания	Среднее время генерации блока; Среднее количество транзакций в системе
[15]	Рассматривается система на примере модели $M/G/1$. Поступление данных в узлы моделируется как неоднородный процесс Пуассона, где распределение скорости поступления на узлы выводится из аналитической модели протокола доставки данных.	Теория массового обслуживания	Вероятности времени распределения блоков и транзакций; Время ответа узла; Вероятность разветвления цепочки; Продолжительность периода несогласованности реестра
[16]	Предлагаются стохастические сетевые модели, чтобы фиксировать эволюцию и динамику развития цепочки блоков. Используется комбинация аналитических расчетов и экспериментов по моделированию для исследования как стационарных, так и переходных характеристик производительности.	Стохастические модели	Влияние задержки распространения блока; Мощность хэширования узлов
[17]	Для моделирования предлагаются игровые теории для решения общих проблем в сети блокчейнов, таких как безопасность, проблемы, связанные с управлением майнингом, а также вопросы, касающиеся экономики блочной цепи.	Теория игр	Экономические аспекты
[18]	Рассматривается система на примере модели $M/G/\infty$. Используется эквивалентность между двумя конкретными дисциплинами обслуживания для получения стационарного распределения модели.	Теория массового обслуживания	Распределение периодов занятости; Задержки при обслуживании
[19]	Развивается теория массового обслуживания в блокчейн-системах и дается оценка производительности системы. Для этого разрабатывается Марковская система очередей пакетного обслуживания с двумя различными этапами, которые подходят для четкого выражения процесса майнинга в пуле майнеров и построения новой цепочки блоков.	Теория массового обслуживания; Марковские процессы	Среднее количество транзакций в очереди; Среднее количество транзакций в блоке; Среднее время подтверждения транзакции

ТАБЛИЦА 2. Решения в области симуляции для блокчейн-систем

TABLE 2. Simulation Solutions for Blockchain Systems

Решение	Описание	Пакеты программ
Тестовые сети	Тестовая сеть определенной системы применяется для проверки работоспособности или значимости приложения. Используются анализаторы монет, которые не имеют реальной стоимости.	Bitcoin testnet explorer; Blockcypher; Testnet explorer; Bitcoin testnet faucet; Rinkeby network; Ganachecli; Ethereum Tester; Truffle framework; Remix ide; Ibm blockchain; Platform extension for visual studio code; Remme; Cryptospaniards
Демонстрация работы технологии	Данные решения показывают, как работают основные операции блокчейна, такие как хеширование, майнинг, распространение, а также позволяют получить сведения о результате процедуры при изменении определенных параметров.	Blockchain demo
Симуляторы для управления событиями	С помощью таких решений пользователи могут изучать основные характеристики и показатели сети, исследовать взаимодействия между узлами и сравнивать различные сценарии моделирования. Они служат справедливым средством сравнения для различных платформ и позволяет глубже понять различные варианты дизайна системы. Решения применяются как предварительное тестирование для оценки общей производительности, и с рабочими нагрузками для оценки производительности отдельных уровней.	Vibes; Simblock; Blocksim; BlockLite; Bitcoin simulator; Blockbench
Симулятор участка сети	Решения объединяют математические и логические аспекты и воспроизводят реальное поведение системы с помощью компьютерного программного обеспечения	AnyLogic; Mathlab; NS3; GPSS

Проверка агрегированной исходной временной последовательности на самоподобие является важной задачей при моделировании данных СМО. Как было определено в [28], самоподобие сохраняется при агрегировании исходной временной последовательности. В данном случае процесс является самоподобным, если:

$$\lim_{n\to\infty} R^n(k) = \frac{\sigma^2}{2}((k+1)^{2H} - 2k^{2H} + (k-1)^{2H}), \quad (2)$$

где $R^n(k)$ – корреляционная функция для агрегированного временного ряда; H – параметр Херста; k – временной сдвиг; σ^2 – выборочная дисперсия последовательности.

Однако если рассматривать ситуацию, когда закон распределения времени обслуживания такого трафика будет описан более сложными к инициализации зависимостями, то стоит перейти к модели с общим видом распределения – *M/G/1*. Тогда, в соответствии с [29], среднее время пребывания пакета в системе определяется по выражению:

$$T = \rho + \rho^2 \frac{1 + C_B^2}{2(1-\rho)}, \quad (3)$$

где ρ – коэффициент использования системы; C_B^2 – нормированная дисперсия времени обслуживания.

Среднее время пребывания в очереди определяется следующим образом:

$$W = \frac{\lambda \ddot{x}^2}{2(1-\rho)}, \quad (4)$$

где λ – средняя интенсивность поступления заявки; $\ddot{x}^2$ – момент второго порядка случайной величины.

Большинство существующих приложений придерживается характера одноадресной передачи, при которой трафик направляется из одного источника к одному получателю. Широковещательная передача применяется для отправки единого потока команд управления и прочей служебной информации всем абонентам сети. Однако из-за специфики работы блокчейн-алгоритма можно отметить существенный рост многоадресной передачи трафика при обновлении данных в реестре, которая дублирует информацию для различных блокчейн-узлов.

В сетях передачи данных имеется много очередей на передачу, которые взаимодействуют друг с другом, происходят слияния с частями других потоков, что влияет и усложняет характер процессов [30]. В связи с чем на граничном маршрутизаторе может организовываться модель взаимодействия – *G/G/1* и *G/G/n*. Однако одним из способов оценки вероятностно-временных характеристик телекоммуникационных узлов инфокоммуникационной сети, как системы массового обслуживания, в условиях слабовыраженных корреляционных связей является решение интегральных уравнений

Линдли. Уделим особое внимание финальной формуле, полученной при выводе уравнения [30]. Так, интегральная функция времени ожидания при любых значениях аргумента:

$$W(y) = \int_{-\infty}^{y} W(y-u)c(u)du. \qquad (5)$$

Из-за сложности самоподобных процессов для расчета их аналитических моделей, как правило, применяются методы имитационного моделирования.

Для проверки адекватности использования систем имитационного моделирования и моделей в качестве инструмента оценки сетевых характеристик предлагается использовать систему имитационного моделирования AnyLogic.

Данная система поддерживает различные подходы к созданию имитационных моделей, позволяет учитывать различные аспекты моделируемой системы с различным уровнем детализации, имеет графический интерфейс [32].

На рисунке 3 представлена AnyLogic модель сети передачи данных при включении в нее блокчейн-технологии.

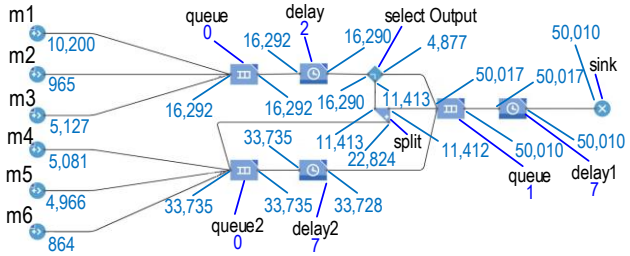

Рис. 3. Моделирование системы с блокчейн-узлами

Fig. 3. Modeling a System with Blockchain Nodes

Эксперимент показал, что работоспособность сети зависит от интенсивности появления заявок, при этом для корректной работы технологии блокчейн представленного типа можно варьировать значения интенсивности узлов и значения размера буфера.

На рисунке 4 представлено сравнение полученных значений при аналитическом моделировании и при имитационном. Данные незначительно различаются, так как при построении моделей автором не учитывались внутренние связи между сетевыми элементами, что могло повлиять на результаты. Также имитационная модель не дает возможности получения точечной оценки исследуемого параметра, а позволяет получить интервальные оценки, точность которых зависит от методов и объема наблюдений, начального состояния, генератора псевдослучайных чисел [30].

Рис. 4. Моделирование системы с блокчейн-технологией

Fig. 4. Modeling a System with Blockchain Technology

Следует отметить, что моделирование производительности технологии блокчейн с помощью системы AnyLogic возможно и удобно для анализа при изменении различных параметров. Однако для более точных результатов необходимо провести дополнительные исследования в области моделирования работы блокчейна на эмуляторе AnyLogic. Анализ моделей показал применимость отдельных систем имитационного моделирования для оценки влияния технологии блокчейн на сети передачи данных.

Заключение

Сегодня объем производимого блокчейн-устройствами трафика меньше объема трафика таких услуг, как передача видео и передача данных, однако из-за растущей популярности технологии потенциально возможное число таких устройств, может стать так велико, что интенсивность производимого ими трафика будет сопоставима с трафиком традиционных услуг. Если трафик блокчейн-технологии обслуживается совместно с критичным к задержке и потерям трафиком, то он может оказывать существенное влияние на качество обслуживания трафика традиционных услуг. В данной работе был проведен и представлен обзор решений в области аналитического и имитационного моделирования с акцентом на системы массового обслуживания. Представлены результаты сравнения моделирования.

В дальнейшем планируется расширить показатели системы для получения более точных результатов при помощи системы AnyLogic и предложить методику расчета сетевой инфраструктуры с учетом характеристик трафика и полученных данных.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90050/19.

Список используемых источников

1. Бородин А.С., Кучерявый А.Е. Сети связи и пандемия // Электросвязь. 2020. № 5. С. 8–10. DOI:10.34832/ELSV.2020.6.5.002

2. Xu X., Pautasso C., Zhu L., Gramoli V., Ponomarev A., Tran A.B., et al. The Blockchain as a Software Connector // Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture (WICSA, Venice, Italy, 5–8 April 2016). IEEE, 2016. PP. 182–191. DOI:10.1109/WICSA.2016.21

3. Palmara P. Tracing and tracking with the blockchain // Tesi di laurea Magistrale. Politecnico di Milano, 2018.

4. Mougayar W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Hoboken: John Wiley & Sons, 2016. 208 p.

5. Elagin V.S., Spirkina A.V., Levakov A., Belozertsev I. Blockchain Behavioral Traffic Model as a Tool to Influence Service IT Security // Future Internet. 2020. Vol. 12. PP. 68. DOI:10.3390/fi12040068

6. Shahid M.N. A Cross-Disciplinary Review of Blockchain Research Trends and Methodologies: Topic Modeling Approach // Proceedings of the 53rd Annual Hawaii International Conference on System Sciences (HICSS, Wailea, Maui, Hawaii, 7–10 January 2020). 2020. PP. 4053–4060. DOI:10.24251/HICSS.2020.495

7. Vladyko A.G., Spirkina A.V., Elagin V.S., Belozertsev I.A., Aptrieva E.A. Blockchain Models to Improve the Service Security on Board Communications // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications (Moscow, Russian, 19–20 March 2020). IEEE, 2020. PP. 1–5. DOI:10.1109/IEEECONF48371.2020.9078572

8. Lao L., Li Z., Hou S., Xiao B., Guo S., Yang Y. A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling // ACM Computing Surveys. 2020. Vol. 53. Iss. 1. DOI:10.1145/3372136

9. Елагин В.С., Спиркина А.В., Владыко А.Г., Иванов Е.И., Помогалова А.В., Аптриева Е.А. Основные сетевые характеристики blockchain трафика и подходы к моделированию // Т-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 4. С. 39–45. DOI:10.36724/2072-8735-2020-14-4-39-45

10. Smetanin S., Ometov A., Komarov M., Masek P., Koucheryavy Y. Blockchain Evaluation Approaches: State-of-the-Art and Future Perspective // Sensors. 2020. № 12. DOI:10.3390/s20123358

11. Ling X., Le Y., Wang J., Ding Z., Gao X. Practical Modeling and Analysis of Blockchain Radio Access Network // IEEE Transactions on Communications. 2020. Vol. 69. Iss. 2. PP. 1021–1037. DOI:10.1109/TCOMM.2020.3029779

12. Memon R.A., Li J., Ahmed J., Khan A., Nazir M.I., Mangrio M.I. Modeling of Blockchain Based Systems Using Queuing Theory Simulation // Processing of the 15th International Computer Conference on Wavelet Active Media Technology and Information (Chengdu, China, 14–16 December 2018). IEEE, 2018. PP. 107–111. DOI:10.1109/ICCWAMTIP.2018.8632560

13. Memon R.A., Li J.P., Ahmed J. Simulation model for blockchain systems using queuing theory // Electronics. 2019. Vol. 8. Iss. 2. DOI:10.3390/electronics8020234

14. Kawase Y., Kasahara S. Transaction-Confirmation Time for Bitcoin: A Queueing Analytical Approach to Blockchain Mechanism // Proceedings of the 12th International Conference on Queueing Theory and Network Applications (QTNA 2017, Qinhuangdao, China, 21–23 August 2017). Lecture Notes in Computer Science. Cham: Springer, 2017. Vol. 10591. PP. 75–88. DOI:10.1007/978-3-319-68520-5_5

15. Mišić J., Mišić V.B., Chang X., Motlagh S.G., Zulfiker M.A. Modeling of Bitcoin's Blockchain Delivery Network // IEEE Transactions on Network Science and Engineering. 2019. Vol. 7. Iss. 3. PP. 1368–1381. DOI:10.1109/TNSE.2019.2928716

16. Papadis N., Borst S., Walid A., Grissa M., Tassiulas L. Stochastic Models and Wide-Area Network Measurements for Blockchain Design and Analysis // Proceedings of the IEEE INFOCOM 2018 – IEEE Conference on Computer Communications (Honolulu, USA, 16–19 April 2018). IEEE, 2018. PP. 2546–2554. DOI:10.1109/INFOCOM.2018.8485982

17. Liu Z., Luong N.C., Wang W., Niyato D., Wang P., Liang Y.-C., Kim D.I. A Survey on Applications of Game Theory in Blockchain // arXiv preprint arXiv:1902.10865. 2019. PP. 1–26.

18. Frolkova M., Mandjes M. A Bitcoin-inspired infinite-server model with a random fluid limit // Stochastic Models. 2019. Vol. 35. Iss. 1. PP. 1–32. DOI:10.1080/15326349.2018.1559739

19. Li Q.L., Ma J.Y., Chang Y.X. Blockchain Queue Theory // Proceedings of the 7th International Conference on Computational Social Networks (CSoNet 2018, Shanghai, China, 18–20 December 2018). Lecture Notes in Computer Science. Cham: Springer, 2018. Vol. 11280. PP. 25–40. DOI:10.1007/978-3-030-04648-4_3

20. Makolkina M., Koucheryavy A., Paramonov A. Investigation of Traffic Pattern for the Augmented Reality Applications // Proceedings of the 15th IFIP WG 6.2 International Conference on Wired/Wireless Internet Communication (WWIC 2017, St. Petersburg, Russia, 21–23 June 2017). Lecture Notes in Computer Science. Cham: Springer, 2017. Vol. 10372. PP. 233–246. DOI:10.1007/978-3-319-61382-6_19

21. Rec. ITU-T. Q.3925 Traffic Flow Types for Testing Quality of Service Parameters on Model Networks. ITU, 2012.

22. Карташевский В.Г. Основы теории массового обслуживания. М.: Горячая линия – Телеком, 2013. 126 с.

23. Хинчин А.Я. Математические методы теории массового обслуживания: труды математического института им. В.А. Стеклова. М.: Изд. АН СССР, 1955, 122 с.

24. Лившиц Б.С., Пшеничинков А.П., Харкевич А.Д. Теория телетрафика. М.: Связь, 1979. 224 с.

25. Шелухин О.И. Мультифракталлы. Инфокоммуникационные приложения. М.: Горячая Линия – Телеком, 2011. 578 с.

26. Викулов А.С., Парамонов А.И. Анализ трафика в сети беспроводного доступа стандарта IEEE 802.11 // Труды учебных заведений связи. 2017. Т. 3. № 3. С. 21–27.

27. Кучерявый А.Е., Махмуд О.А., Парамонов А.И. Метод маршрутизации трафика в сети интернета вещей на основе минимума вероятности коллизий // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 37–44. DOI:10.31854/1813-324X-2019-5-3-37-44

28. Назаров А.Н., Сычев К.И. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. Красноярск: Полиздат, 2010. 390 с.

29. Клейнрок Л. Вычислительные сети с очередями. М.: Мир, 1979. 600 с.
30. Парамонов А.И. Разработка и исследование комплекса моделей трафика для сетей связи общего пользования. Автореф. дис. … докт. техн. наук. СПб: СПбГУТ, 2014.
31. Самуйлов К.Е. Методы анализа и расчета сетей сигнализации и мультисервисных сетей с одноадресными и многоадресными соединениями. Автореф. дис. … докт. техн. наук. Москва: МТУСИ, 2005.
32. Spirkina A.V., Aptrieva E.A., Elagin V.S., Shvidkiy A.A., Savelieva A.A. Approaches to Modeling Blockchain Systems // Proceedings of the 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (Brno, Czech Republic, 5–7 October 2020). IEEE, 2020. PP. 242–247. DOI:10.1109/ICUMT51630.2020.9222437

* * *

Scientific Aspects of Structural and Parametric Simulation Modeling of Blockchain Systems

A. Spirkina[1]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-1-122-131
Received 10th February 2021
Accepted 15th March 2021

For citation: Spirkina A. Scientific Aspects of Structural and Parametric Simulation Modeling of Blockchain Systems. *Proc. of Telecom. Universities.* 2021;7(1):122–131. (in Russ.) DOI:10.31854/1813-324X-2021-7-1-122-131

Abstract: *Over the past decade, in addition to multiservice networks, blockchain technology has undergone significant development due to the possibility of organizing a safe, integral, reliable exchange and storage of information. Due to the great demand for the technology, there is a problem of data transmission to the operators' networks. At the same time, a key task appears to consider the effect of this technology on network characteristics to predict traffic behavior on the network and ensure the required service quality indicators, as well as the stability of the state of the public communication network elements when the distributed ledger technology is operating. However, to consider and analyze the influence of technology in a full-scale experiment is a labor-intensive task that cannot always be performed, therefore, in this article, the authors propose to consider approaches to structural-parametric modeling of these systems.*

Keywords: *blockchain, distributed ledger, decentralized systems, simulation, analytical modeling.*

FUNDING

The reported study was funded by RFBR according to the research project № 19-37-90050/19.

References

1. Borodin A.S., Koucheryavy A.Eu. Communications Networks and Pandemic. *Elektrosvyaz.* 2020;5:8–10. DOI:10.34832/ELSV.2020.6.5.002 (in Russ.)
2. Xu X., Pautasso C., Zhu L., Gramoli V., Ponomarev A., Tran A.B., et al. The Blockchain as a Software Connector. *Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture, WICSA, 5–8 April 2016, Venice, Italy*. IEEE; 2016. p.182–191. DOI:10.1109/WICSA.2016.21
3. Palmara P. Tracing and tracking with the blockchain. *Tesi di laurea Magistrale*. Politecnico di Milano; 2018.
4. Mougayar W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Hoboken: John Wiley & Sons; 2016. 208 p.
5. Elagin V.S., Spirkina A.V., Levakov A., Belozertsev I. Blockchain Behavioral Traffic Model as a Tool to Influence Service IT Security. *Future Internet*. 2020;12:68. DOI:10.3390/fi12040068
6. Shahid M.N. A Cross-Disciplinary Review of Blockchain Research Trends and Methodologies: Topic Modeling Approach. *Proceedings of the 53rd Annual Hawaii International Conference on System Sciences, HICSS, 7–10 January 2020, Wailea, Maui, Hawaii*. 2020. p.4053–4060. DOI:10.24251/HICSS.2020.495
7. Vladyko A.G., Spirkina A.V., Elagin V.S., Belozertsev I.A., Aptrieva E.A. Blockchain Models to Improve the Service Security on Board Communications. *2020 Systems of Signals Generating and Processing in the Field of on Board Communications, 19–20 March 2020, Moscow, Russian*. IEEE; 2020. p.1–5. DOI:10.1109/IEEECONF48371.2020.9078572

8. Lao L. Li Z., Hou S., Xiao B., Guo S., Yang Y. A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling. *ACM Computing Surveys*. 2020;53(1). DOI:10.1145/3372136

9. Elagin V.S., Spirkina A.V., Vladyko A.G., Ivanov E.I., Pomogalova A.V., Aptrieva E.A. The Main Network Characteristics of Blockchain Traffic and Modeling Approaches. *T-Comm*. 2020;4:39–45. (in Russ.) DOI:10.36724/2072-8735-2020-14-4-39-45

10. Smetanin S., Ometov A., Komarov M., Masek P., Koucheryavy Y. Blockchain Evaluation Approaches: State-of-the-Art and Future Perspective. *Sensors*. 2020;12. DOI:10.3390/s20123358

11. Ling X., Le Y., Wang J., Ding Z., Gao X. Practical Modeling and Analysis of Blockchain Radio Access Network. *IEEE Transactions on Communications*. 2020;69(2):1021–1037. DOI:10.1109/TCOMM.2020.3029779

12. Memon R.A., Li J., Ahmed J., Khan A., Nazir M.I., Mangrio M.I. Modeling of Blockchain Based Systems Using Queuing Theory Simulation. *Processing of the 15th International Computer Conference on Wavelet Active Media Technology and Information, 14–16 December 2018, Chengdu, China*. IEEE; 2018. p.107–111. DOI:10.1109/ICCWAMTIP.2018.8632560

13. Memon R.A., Li J.P., Ahmed J. Simulation model for blockchain systems using queuing theory. *Electronics*. 2019;8(2). DOI:10.3390/electronics8020234

14. Kawase Y., Kasahara S. Transaction-Confirmation Time for Bitcoin: A Queueing Analytical Approach to Blockchain Mechanism. *Proceedings of the 12th International Conference on Queueing Theory and Network Applications, QTNA 2017, 21–23 August 2017, Qinhuangdao, China. Lecture Notes in Computer Science*. Cham: Springer; 2017. vol.10591. p.75–88. DOI:10.1007/978-3-319-68520-5_5

15. Mišić J., Mišić V.B., Chang X., Motlagh S.G., Zulfiker M.A. Modeling of Bitcoin's Blockchain Delivery Network. *IEEE Transactions on Network Science and Engineering*. 2019;7(3):1368–1381. DOI:10.1109/TNSE.2019.2928716

16. Papadis N., Borst S., Walid A., Grissa M., Tassiulas L. Stochastic Models and Wide-Area Network Measurements for Blockchain Design and Analysis. *Proceedings of the IEEE INFOCOM 2018 – IEEE Conference on Computer Communications, 16–19 April 2018, Honolulu, USA*. IEEE; 2018. p.2546–2554. DOI:10.1109/INFOCOM.2018.8485982

17. Liu Z., Luong N.C., Wang W., Niyato D., Wang P., Liang Y.-C., Kim D.I. A Survey on Applications of Game Theory in Blockchain. *arXiv preprint arXiv:1902.10865*. 2019. p.1–26.

18. Frolkova M., Mandjes M. A Bitcoin-inspired infinite-server model with a random fluid limit. *Stochastic Models*. 2019;35(1):1–32. DOI:10.1080/15326349.2018.1559739

19. Li Q.L., Ma J.Y., Chang Y.X. Blockchain Queue Theory. *Proceedings of the 7th International Conference on Computational Social Networks, CSoNet 2018, 18–20 December 2018, Shanghai, China. Lecture Notes in Computer Science*. Cham: Springer; 2018. vol.11280. p.25–40. DOI:10.1007/978-3-030-04648-4_3

20. Makolkina M., Koucheryavy A., Paramonov A. Investigation of Traffic Pattern for the Augmented Reality Applications. *Proceedings of the 15th IFIP WG 6.2 International Conference on Wired/Wireless Internet Communication, WWIC 2017, 21–23 June 2017, St. Petersburg, Russia. Lecture Notes in Computer Science*. Cham: Springer; 2017. vol.10372. p.233–246. DOI:10.1007/978-3-319-61382-6_19

21. Rec. ITU-T. Q.3925 *Traffic Flow Types for Testing Quality of Service Parameters on Model Networks*. ITU; 2012.

22. Kartashevskij V.G. *Basics of Queuing Theory*. Moscow: Goryachaya liniya – Telekom Publ.;2013. 126 p. (in Russ.)

23. Hinchin A.Ya. *Mathematical Methods of the Theory of Queuing: Proceedings of the Mathematical Institute named after V.A. Steklov*. Moscow: Academy of Sciences of the USSR Publ.; 1955. 122 p. (in Russ.)

24. Livshic B.S., Pshenichinkov A.P., Kharkevich A.D. *Teletraffic Theory*. Moscow: Svyaz Publ.; 1979. 224 p. (in Russ.)

25. Sheluhin O.I. *Multifractals. Infocommunication Applications*. Moscow: Goryachaya Liniya – Telekom; 2011. 578 p. (in Russ.)

26. Vikulov A., Paramonov A. IEEE 802.11 WLAN Traffic Analysis. *Proc. of Telecom. Universities*. 2017;3(3):21–27. (in Russ.)

27. Koucheryavy A., Mahmood O.A., Paramonov A. Traffic Routing Method for the Internet of Things Based on the Minimum of Collisions Probability. *Proc. of Telecom. Universities*. 2019;5(3):37–44. (in Russ.) DOI:10.31854/1813-324X-2019-5-3-37-44

28. Nazarov A.N., Sychev K.I. *Models and Methods for Calculating Performance Indicators of Nodal Equipment and Structural and Network Parameters of Next Generation Communication Networks*. Krasnoyarsk: Poliizdat Publ.; 2010. 390 p. (in Russ.)

29. Klejnrok L. *Computing Networks with Queues*. Moscow: Mir Publ.; 1979. 600 p. (in Russ.)

30. Paramonov A.I. *Development and Research of a Complex of Traffic Models for Public Communication Networks.* D.Sc Thesis. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications; 2014. (in Russ.)

31. Samujlov K.E. *Methods for Analysis and Calculation of Signaling Networks and Multiservice Networks with Unicast and Multicast Connections*. D.Sc Thesis. Moscow: Moscow Technical University of Communications and Informatics; 2005. (in Russ.)

32. Spirkina A.V., Aptrieva E.A., Elagin V.S., Shvidkiy A.A., Savelieva A.A. Approaches to Modeling Blockchain Systems. *Proceedings of the 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, 5–7 October 2020, Brno, Czech Republic*. IEEE; 2020. p.242–247. DOI:10.1109/ICUMT51630.2020.9222437

Сведения об авторе:

СПИРКИНА Анастасия Валентиновна

аспирант кафедры Инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, spirkina.av@gmail.com

https://orcid.org/0000-0002-9047-1484