СЕКЦИЯ 6

УПРАВЛЕНИЕ РАЗВИТИЕМ БАНКОВСКИХ И ФИНАНСОВЫХ СИСТЕМ

DOI: 10.25728/mlsd.2023.0682

ВЫЧИСЛИТЕЛЬНАЯ ОЦЕНКА ОПЕРАЦИОННОЙ АРХИТЕКТУРЫ ЦИФРОВОЙ ВАЛЮТЫ ЦЕНТРАЛЬНОГО БАНКА НА ОСНОВЕ HYPERLEDGER FABRIC

Албычев А.С.
Федеральное казначейство Министерства финансов Российской Федерации, Москва, Россия; МИРЭА – Российский технологический университет, Москва, Россия
albychev@mirea.ru
Ильин Д.Ю., Никульчев Е.В.
МИРЭА – Российский технологический университет, Москва, Россия
i@dmitryilin.com, nikulchev@mail.ru

Аннотация. Цифровая валюта центрального банка является виртуальной валютой, эквивалентной национальным валютам, которая централизованно управляется государством. В настоящее время многие страны проводят исследования технологий цифровых валют. Рассмотрены вычислительные оценки операционной архитектуры цифровой валюты, сформированной на основе технологий распределенного реестра и Hyperledger Fabric.

Ключевые слова: Цифровая валюта центрального банка, операционная архитектура, технологии распределенного реестра.

Введение

В настоящее время инновационными формами денежных операции являются мобильные платежи и использование виртуальных валют. С помощью портативных устройств – от смартфонов до часов имеется возможность оплачивать товары и услуги, отправлять денежные суммы частным лицам. Виртуальные валюты, начиная с Биткойн, становятся в определенном смысле денежными средствами, но не имеют своего физического воплощения в чеканных монетах или напечатанных бумагах, существуя только в виртуальном мире. Однако Биткойн, в отличии от бумажной валюты, не контролируется централизованно и не обеспечен государством.

Цифровая валюта центрального банка (central bank digital currencies, ЦВЦБ) – это цифровая версия национальной валюты, то есть денежная расчетная единица эквивалентная национальной валюте. Национальный Центральный банк выпускает и контролирует ЦВЦБ [1]. Многие страны проводят исследования о возможности внедрения ЦВЦБ [2], в том числе и цифровой евро. Многие изучают экосистему ЦВЦБ, которая предполагает сотрудничество с частным сектором и функциональную совместимость с существующими платежными системами.

Блокчейн и технология распределенного реестра (DLT) — это набор технологий и протоколов, которые используются распределенными участниками для коллективного и безопасного обслуживания децентрализованной цифровой базы данных без единого центрального управления. Биткойн – самое известное применение DLT [3], другим примером является Эфириум [3]. Разработчики могут использовать Эфириум в качестве платформы для создания множества инновационных криптовалют. Отличные от Биткойна и Эфириума криптовалюты называются «Альткойны».

Участвующие в денежной операции с цифровой валютой имеют возможность наблюдать и подтверждать транзакции, однако именно Центральные банки выбирают подходящую DLT-платформу для реализации и операционную архитектуру.

Существует целый ряд DLT-платформ, рассматриваемых как основа для ЦВЦБ. Corda [4] – это DLT с открытым исходным кодом, платформа, которая обеспечивает строгую конфиденциальность для записи и управление контрактами между сторонами. Corda уникальна среди блокчейн-платформ, которые вводят концепция «нотариуса», который «ставит печать» на каждой сделке. Hyperledger Fabric [5] – DLT-основа для разработки приложений или модульных архитектурных решений. Quorum [6] – DLT на основе Ethereum, который содержит расширения для улучшения

взаимодействия между сторонами. Hyperledger Iroha [7] – DLT с новым отказоустойчивым консенсусом алгоритм под названием YAC [8]. Hyperledger Besu [9] – это корпоративный клиент Ethereum для публичных и частных разрешенные сети. Hyperledger Besu включает в себя несколько алгоритмов консенсуса и имеет комплексные схемы разрешений, специально разработанные для использования в консорциуме. Elements [10] – это блокчейн-платформа с открытым исходным кодом, обеспечивающая доступ к разработанным сообществом функциям, таким как конфиденциальные транзакции. Также существуют и специализированные протоколы, например, Interledger [11] открытый протокол для отправки платежей по различным реестрам.

Для реализации ЦВЦБ рассматриваются различные операционные архитектуры. Одна из них, приведенная на рис. 1 [12], подразумевает распределение данных цифровой валюты на сегменты и передачу ресурсоемких вычислений операторам ЦВЦБ. Для обеспечения надежности и неподдельности операций в рамках сегмента они могут распределяться между несколькими операторами.

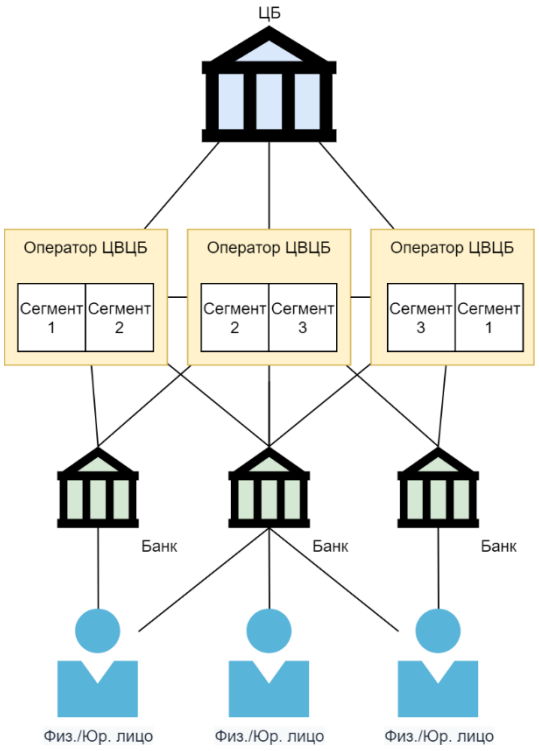

Рис. 1. Операционная архитектура ЦВЦБ

В докладе рассматривается технология Hyperledger Fabric версии 2.4 в качестве реализации одного из сегментов в рамках операционной архитектуры, приведенной на рис. 1.

1. Эксперимент

Обработка транзакций в блокчейн-сетях является ресурсоемкой задачей. Производительность сети сильно зависит от конфигурации, алгоритма консенсуса и количества участников, вовлеченных в процесс обработки транзакции. В Hyperledger Fabric процесс формирования новых блоков выведен в отдельную службу упорядочения (СУ), но, прежде чем транзакция будет передана в нее, требуется одобрение заданным количеством организаций-участников блокчейн-сети, что выполняется одноранговыми узлами (ОУ). Одним из вариантов является одобрение большинством, когда большая часть организаций должна подтвердить корректность транзакции. Предполагается, что чем больше узлов должны одобрить транзакцию, тем надежнее будет результат. Однако, уместным будет предположение, что чем больше узлов вовлечено в процесс одобрения транзакции, тем менее производительной будет система в целом.

1.1. Вычислительная инфраструктура

Важно отметить, что для эксперимента по оценке производительности блокчейн-сети требуется подходящее оборудование. Ввиду того, что количество ВМ для задачи измеряется десятками, для

проведения исследования было использовано оборудование [13] с характеристиками, представленными в таблице 1.

Таблица 1. Характеристики хост-системы для экспериментального стенда

Элемент конфигурации	**Характеристика**
Тип процессора	Intel Xeon E5-2697 v4 @ 2.30ГГц
Виртуальные ядра процессора	70 (35 на сокет)
Объем ОЗУ	74 Гб
Тип жесткого диска	HDD
Объем дискового пространства	470 Гб
Гипервизор	ESXi 7.0 Update 3

Для обеспечения доступа к внешней сети, а также для присвоения IP-адресов виртуальным машинам, была создана отдельная сервисная виртуальная машина с характеристиками, представленными в таблице 2. На ней были установлены и сконфигурированы службы NAT и DHCP.

Таблица 2. Характеристики сервисной виртуальной машины

Элемент конфигурации	**Характеристика**
Виртуальные ядра процессора	2
Объем ОЗУ	4 Гб
Объем дискового пространства	50 Гб, динамический (thin provisioned)
Операционная система	Windows Server 2016

Для программного управления экспериментальным стендом была подготовлена виртуальная машина с пользовательским интерфейсом. Основные характеристики ВМ приведены в таблице 3. На нее также было установлено следующее программное обеспечение:

- модифицированная версия инструмента Repexlab для работы с гипервизором VMWare ESXi;
- Vagrant с плагином vagrant-vmware-esxi;
- утилита ovftool.

Таблица 3. Характеристики виртуальной машины управления экспериментальным стендом

Элемент конфигурации	**Характеристика**
Виртуальные ядра процессора	4
Объем ОЗУ	4 Гб
Объем дискового пространства	90 Гб, динамический (thin provisioned)
Операционная система	Ubuntu 22.04

1.2. Конфигурация виртуального экспериментального стенда

Для создания виртуального экспериментального стенда была подготовлена базовая ВМ, которая затем программным способом клонировалась для создания всех программно-управляемых ВМ, представленных на рис. 2.

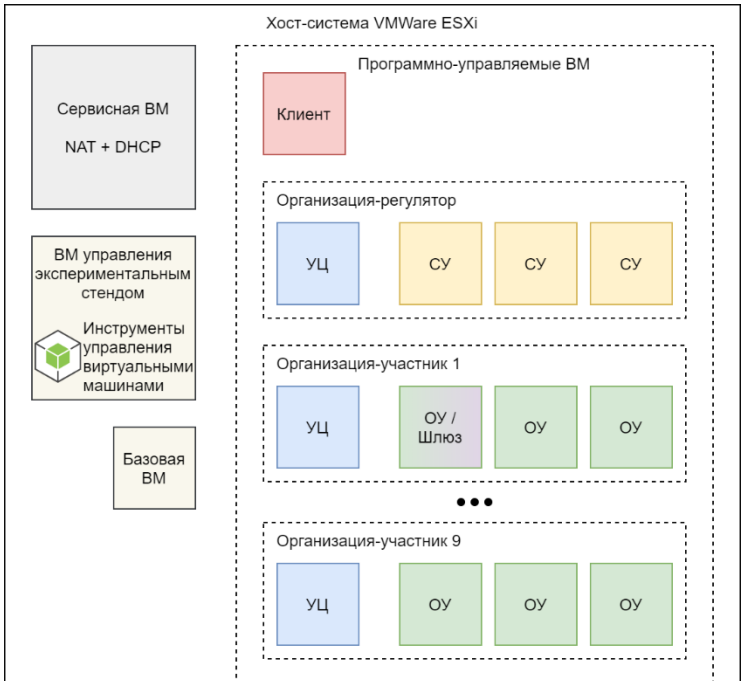

Рис. 2. Конфигурация виртуальных машин экспериментального стенда

Экспериментальный стенд состоит из 41 ВМ, характеристики которых приведены в таблице 4. В нем представлено 9 групп ВМ, обозначающих организации-участники, одну группу ВМ, соответствующую организации-регулятору, и отдельную виртуальную машину Клиент, необходимую для формирования нагрузки.

Таблица 4. Характеристики программно-управляемых виртуальных машин экспериментального стенда

Элемент конфигурации	**Характеристика**
Виртуальные ядра процессора	1 (4 для ВМ Клиент)
Объем ОЗУ	1 Гб (2 Гб для ВМ Клиент)
Объем дискового пространства	10 Гб, динамический (thin provisioned)
Операционная система	Ubuntu 20.04
Инструмент мониторинга ресурсов	atop (интервал – 10 секунд)

1.3. Алгоритм эксперимента

Для эксперимента был подготовлен алгоритм, представленный на рис. 3. Он состоит из подготовительного этапа и этапа, на котором выполняется оценка конкретных конфигураций блокчейн-сети. На вход подаются конфигурации виртуальных машин (их характеристик и программного обеспечения), конфигурации блокчейн-сети и конфигурации для инструмента проведения нагрузочных испытаний. Результатом выполнения алгоритма является два набора отчетов: отчеты, сформированные инструментом проведения нагрузочных испытаний и отчеты об использовании вычислительных ресурсов.

При запуске эксперимента производится создание всех ВМ и их базовое конфигурирование – установка и настройка программного обеспечения. Затем, состояние всех ВМ фиксируется и для них создаются снапшоты средствами гипервизора. Далее, алгоритм переходит к работе с различными конфигурациями блокчейн-сети, которая формируется из ***n*** одноранговых узлов и ***m*** организаций. Для каждого из сочетаний производится следующее:

- виртуальные машины возвращаются в исходное состояние;
- производится синхронизация времени;
- осуществляется конфигурирование блокчейн-сети с заданным количеством ОУ и организаций;
- осуществляется подготовка инструмента генерации нагрузки;

- проводится серия нагрузочных испытаний с различными паттернами нагрузки, после каждой из которых формируется отчет и составляются отчеты об использовании вычислительных ресурсов каждой ВМ.

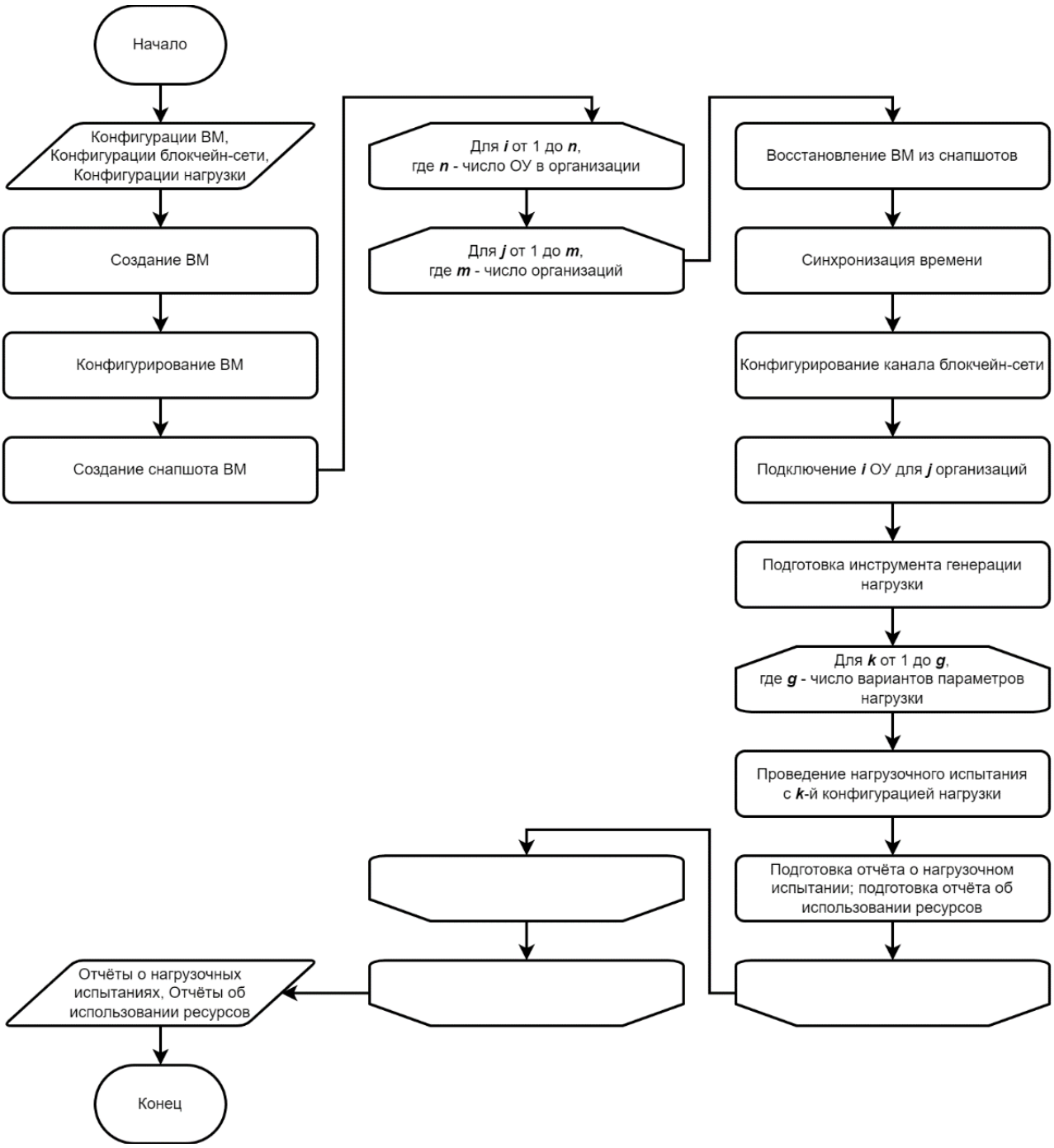

Рис. 3. Алгоритм программно-управляемого эксперимента

На рис. 4 наглядно представлен состав формируемой блокчейн-сети. Количество организаций и одноранговых узлов изменяется, тогда как остальные параметры остаются неизменны. Для всех сочетаний канал Hyperledger Fabric настраивался с правилом одобрения транзакции MAJORITY, т.е. в подтверждении корректности транзакции должна участвовать большая часть организаций в блокчейн-сети.

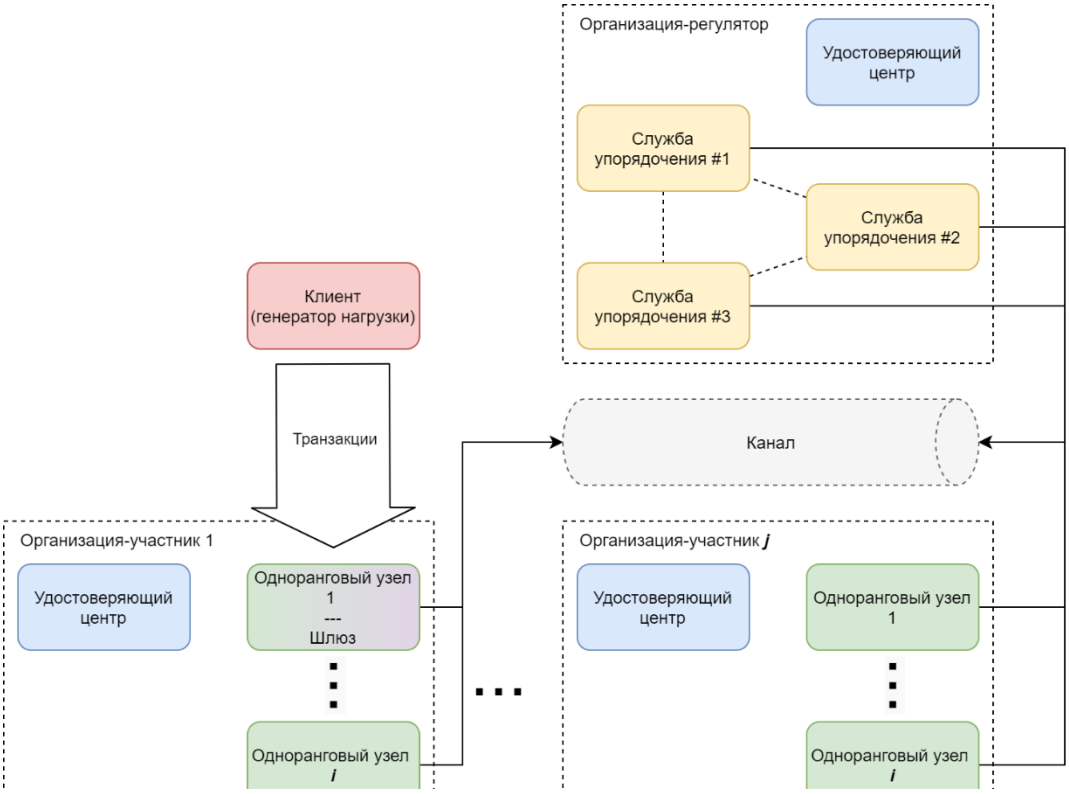

Рис. 4. Конфигурация блокчейн-сети

2. Результаты

Нагрузочные испытания проводились с помощью Hyperledger Caliper в режиме «fixed-load», с 4 процессами нагрузки с общей нагрузкой в 10, 100 и 1000 транзакций в секунду. Нагрузка производилась в течение 3 минут для каждого режима. Каждая транзакция генерируемая Hyperledger Caliper выполняла следующие действия:

- выбор двух случайных аккаунтов (отправителя и получателя) из списка;
- запрос баланса отправителя;
- запрос на передачу 10% от текущего баланса получателю.

Далее будут рассмотрены результаты для максимальной нагрузки, т.е. 1000 транзакций в секунду. В таблице 5 приведены полученные оценки пропускной способности и задержки при выполнении транзакций для всех рассмотренных сочетаний числа ОУ в организации и организаций.

Таблица 5. Результаты нагрузочных испытаний

Одноранговые узлы в организации	**Организации-участники**	**Пропускная способность (TPS)**	**Максимальная задержка (сек)**	**Минимальная задержка (сек)**	**Средняя задержка (сек)**
1	1	294,7	7,96	0,01	1
1	2	217,8	11,23	0,01	1,11
1	3	198,2	12,38	0,01	1,26
1	4	188,9	14,95	0,01	1,64
1	5	163,5	16,81	0,01	1,98
1	6	158,2	16,98	0,02	2,31
1	7	122,4	19,92	0,01	2,19
1	8	129,8	29,41	0,01	2,8
1	9	69,1	64,27	0,02	4,47
2	1	285	10,03	0,01	0,99
2	2	219,7	14,51	0,01	1,12
2	3	171,7	13,01	0,01	1,37
2	4	169	15,1	0,01	1,28
2	5	125	22,65	0,02	2,57
2	6	129,8	19,3	0,01	1,69

Одноранговые узлы в организации	Организации-участники	Пропускная способность (TPS)	Максимальная задержка (сек)	Минимальная задержка (сек)	Средняя задержка (сек)
2	7	100,5	32,04	0,01	2,2
2	8	97,4	26,27	0,02	2,88
2	9	64,4	47,96	0,03	3,36
3	1	217,6	10,34	0,01	1,24
3	2	198,1	16,86	0,01	1,21
3	3	162,5	17	0,01	1,79
3	4	166,9	15,54	0,01	1,49
3	5	114,9	27,31	0,01	2,2
3	6	100,3	23,58	0,01	2,41
3	7	75,9	31,57	0,02	4,18
3	8	78,1	34,96	0,01	2,85
3	9	50,4	49,63	0,01	3,47

Из полученных оценок видно, что с увеличением числа организаций-участников сокращается пропускная способность блокчейн-сети. Для определения узлов, производительность которых зависит от числа организаций, был проведен анализ данных мониторинга ресурсов. При анализе данных учитывались только виртуальные машины, участвующие в блокчейн-сети. Они были объединены в следующие группы:

- Клиент
- Шлюз
- Служба упорядочения
- Одноранговые узлы
- Одноранговые узлы без учета шлюза
- Удостоверяющие центры

По каждой группе были получены средние показатели использования вычислительных ресурсов ЦП, дисковой подсистемы и сетевых подключений. Показатели были нормированы относительно числа транзакций. Таким образом, по следующей формуле была получена оценка ресурсов, затрачиваемых для обработки 1 транзакции:

$$TxCost = MeanLoad/TPS, \quad (1)$$

где $MeanLoad$ – это использование ресурса в секунду (усредненное по виртуальным машинам из группы), а TPS – это количество выполненных транзакций в секунду.

На рис. 5-8 приведены графики использования вычислительных ресурсов для обработки одной транзакции в зависимости от количества организаций в блокчейн-сети при 3 ОУ в каждой организации.

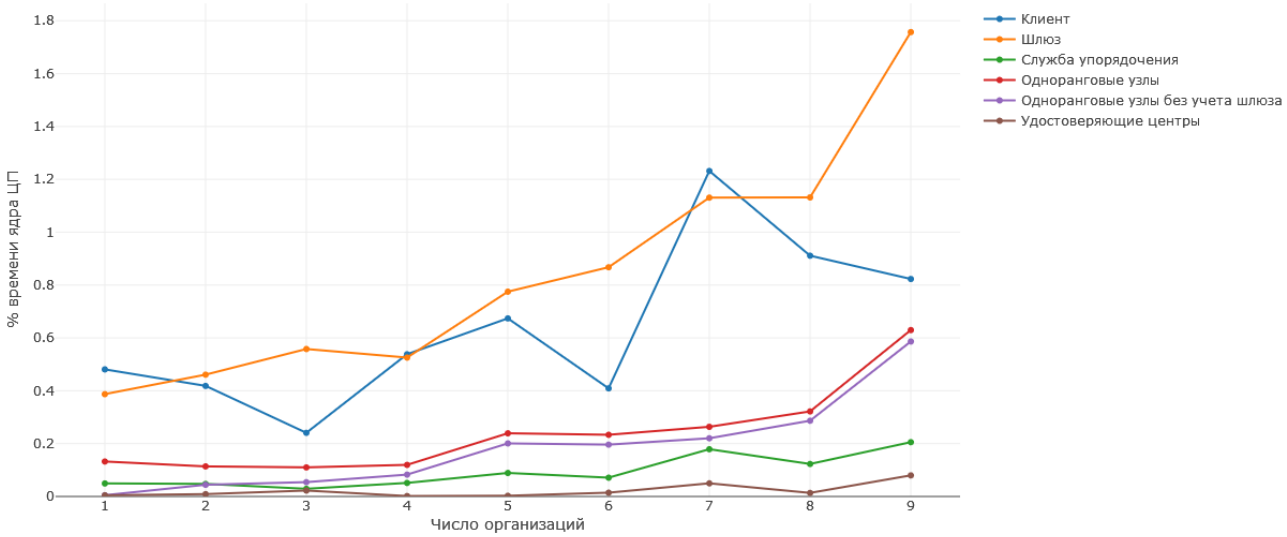

Рис. 5. Связь использованного времени ЦП для обработки одной транзакции с количеством организаций в блокчейн-сети

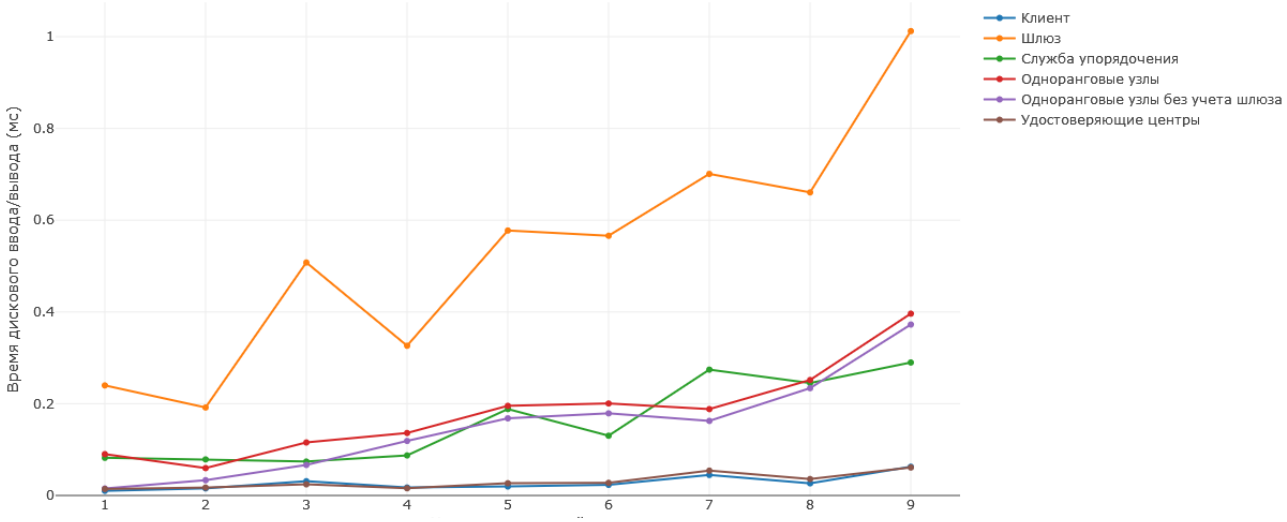

Рис. 6. Связь использованного времени дисковой подсистемы для обработки одной транзакции одноранговым узлом с количеством организаций в блокчейн-сети

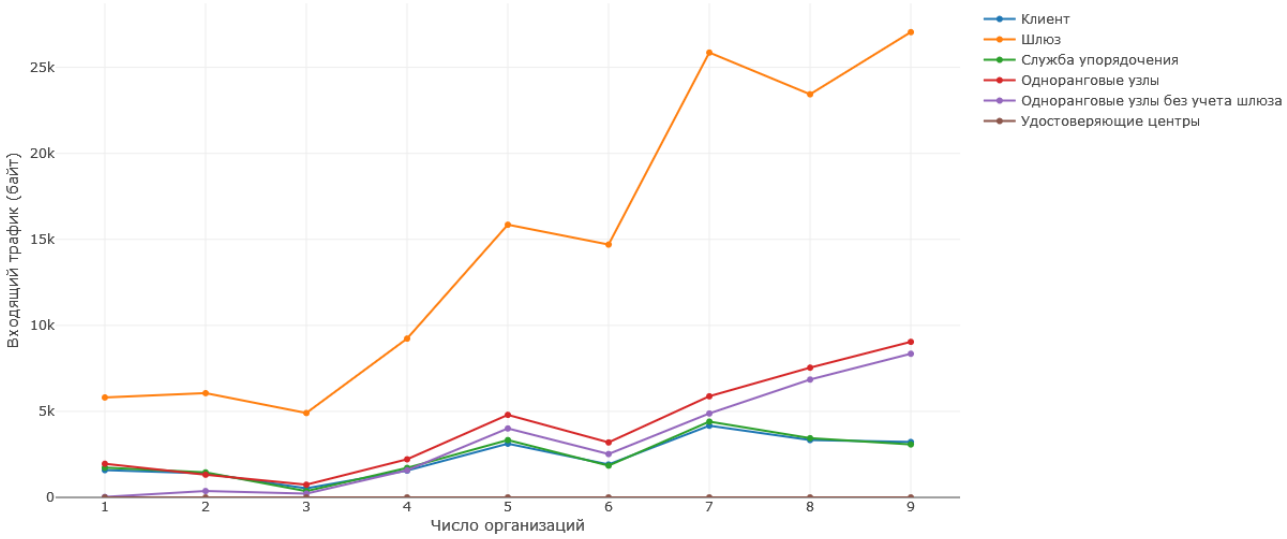

Рис. 7. Связь использованного объема входящего сетевого трафика для обработки одной транзакции с количеством организаций в блокчейн-сети

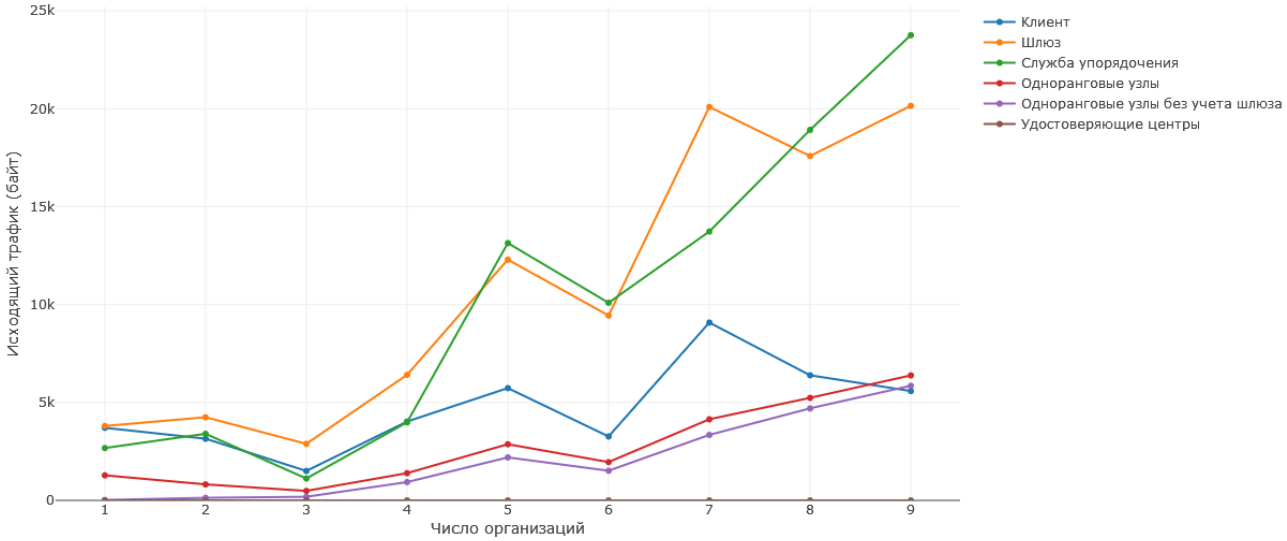

Рис. 8. Связь использованного объема исходящего сетевого трафика для обработки одной транзакции с количеством организаций в блокчейн-сети

Из рис. 5-8 видно, что узел, выполняющий роль шлюза, требователен к ЦП. При этом отмечается значительный прирост используемых ресурсов ЦП с увеличением числа организаций в блокчейн-сети. Количество организаций увеличивает объем трафика, требуемый для обработки транзакций, для большинства узлов, за исключением удостоверяющих центров. Узлы службы упорядочения значительно более требовательны к пропускной способности сетевого канала для исходящего трафика, чем для входящего.

3. Заключение

В работе были рассмотрены актуальные технологии распределенного реестра. Подготовлена вычислительная инфраструктура и виртуальный стенд для оценки Hyperledger Fabric для выбранной операционной архитектуры.

Был задан алгоритм эксперимента, в соответствии с которым была произведена серия нагрузочных испытаний. Результаты показывают снижение производительности блокчейн-сети с увеличением числа организаций, выполняющих обработку транзакций.

Получены оценки использования ресурсов центрального процессора, дисковой подсистемы и сетевых каналов для обработки одной транзакции в зависимости от количества организаций в блокчейн-сети.

Литература

1. *Албычев А.С., Ильин Д.Ю., Никульчев Е.В., Магомедов Ш.Г.* Разработка методики экспериментального исследования технологического обеспечения цифровой валюты центрального банка. // Вестник Рязанского государственного радиотехнического университета. – 2022. N 82. – С. 136–146.
2. *Tronnier F., Harborth D., Biker P.* Applying the extended attitude formation theory to central bank digital currencies // Electronic Markets. – 2023. – Vol. 33. – N 1. – P. 13.
3. *Sethaput V., Innet S.* Blockchain application for central bank digital currencies (CBDC) // Cluster Computing. – 2023. – P. 1-15.
4. Corda Permissioned Distributed Ledger Technology (DLT) // R3 [Online] Available: https://r3.com/products/corda/ (accessed at: 27.05.2023)
5. Hyperledger Fabric // Hyperledger Foundation [Online] Available: https://www.hyperledger.org/use/fabric (accessed at: 27.05.2023)
6. ConsenSys Quorum // ConsenSys [Online] Available: https://consensys.net/quorum/ (accessed at: 27.05.2023)
7. Hyperledger Iroha // Hyperledger Foundation [Online] Available: https://www.hyperledger.org/use/iroha (accessed at: 27.05.2023)
8. *Muratov F., Lebedev A., Iushkevich N., Nasrulin B., Takemiya M.* YAC: BFT Consensus Algorithm for Blockchain // Soramitsu [Online]. Available: https://arxiv.org/pdf/1809.00554.pdf (accessed at: 27.05.2023)
9. Hyperledger Besu // Hyperledger Foundation [Online] Available: https://www.hyperledger.org/use/besu (accessed at: 27.05.2023)
10. Elements // elementsproject.org [Online] Available: https://elementsproject.org/ (accessed at: 27.05.2023)
11. Interledger Protocol (ILP): Open and Inclusive Payments // Interledger Foundation [Online] Available: https://interledger.org/ (accessed at: 27.05.2023)
12. *Албычев А.С., Кудж С.А.* Среда исследований операционно-вычислительной архитектуры информационного обеспечения цифровой валюты центрального банка. // Russian Technological Journal. – 2023. – Т. 11. – N 3. – С. 7-16.
13. *Албычев А.С., Ильин Д.Ю.* Выбор стека технологий вычислительной инфраструктуры для экспериментальных исследований цифровых валют // International Journal of Open Information Technologies. – 2023. – Т. 11. – N 4. – С. 95-101.