На правах рукописи



ЕСЬКОВ Станислав Сергеевич

СПЕЦИАЛЬНОЕ МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЗАИМНОГО ИНФОРМАЦИОННОГО СОГЛАСОВАНИЯ В СИСТЕМАХ РАСПРЕДЕЛЕННОГО РЕЕСТРА

Специальность 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Воронеж – 2020

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Воронежский государственный технический университет».

Научный руководитель: **Кравец Олег Яковлевич,** доктор технических наук, профессор

Официальные оппоненты: **Перепелкин Дмитрий Александрович,** доктор технических наук, профессор, ФГБОУ ВО «Рязанский государственный радиотехнический университет», профессор кафедры систем автоматизированного проектирования вычислительных средств

Соляник Сергей Анатольевич, кандидат технических наук, Воронежский филиал ФГАОУ ДПО "Академия стандартизации, метрологии и сертификации (учебная)", заместитель директора

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева» (г. Красноярск)

Защита состоится «02» октября 2020 года в 14:00 часов в конференц-зале на заседании диссертационного совета Д 212.037.13, созданного на базе ФГБОУ ВО «Воронежский государственный технический университет», по адресу: 394026, г. Воронеж, Московский просп., д. 14.

С диссертацией можно ознакомиться в научно-технической библиотеке ФГБОУ ВО «Воронежский государственный технический университет» и на сайте www.cchgeu.ru.

Автореферат разослан «24» августа 2020 г.

Ученый секретарь
диссертационного совета Гусев Константин Юрьевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Актуальным направлением совершенствования технологий распределенных программных систем является исследование возможностей использования в их архитектуре концепций и технологических решений на базе распределенного реестра (distributed ledger technology – DLT). Особенностью DLT является децентрализация процесса хранения данных, создания множества равнозначных копий этих данных и синхронизации этих копий на основе класса алгоритмов взаимного информационного согласования (ВИС).

К алгоритмам ВИС предъявляются требования по отказоустойчивости и учету возможности нештатного функционирования отдельных узлов. В программном обеспечении практических реализаций DLT-систем, например, таких, как платежные peer-to-peer системы, используется технология цепочки блоков (в терминах DLT-систем - blockchain), в общем случае удовлетворяющая перечисленным выше требованиям.

Большой вклад в совершенствование средств математического и программного обеспечения DLT-систем в целом и систем с распределенным реестром на основе цепочки блоков (DLT ЦБ систем) в частности внесли Л. Лампорт, Д. Фишер, А. Линч, С. Патерсон, Д. Онгаро, Д. Оустерхаут, Р. Шостак, М. Пиз, С. Накамото, Г. Вуд, Д. Вилк, В. Бутерин.

Однако большинство полученных результатов исследований в данной области не в полной мере учитывают в рамках решения задачи ВИС, одновременную реализацию узлами нескольких нештатных функций, таких, например, как формирование ответвления обрабатываемых данных (fork версии) и атаку временной блокировки (сокрытие сгенерированного блока от других узлов системы). Так, в программном обеспечении платежных peer-to-peer систем узлы стремятся увеличить свою эффективность при выполнении алгоритма ВИС путем изменения поведения: выбора между работой по заданным правилам и нештатным функционированием, таким образом определяя стратегию поведения. При этом учет вариантов стратегий поведения узлов или не выполняется, или для них используются проприетарные алгоритмы, специфические для конкретной реализации DLT ЦБ системы и учитывающие варианты стратегии поведения узла только по отдельности. Кроме того, возможность объединения узлов в группы приводит к централизации распределенной системы, что негативно влияет на стабильность ее работы – вероятность формирования единой ЦБ. Централизация увеличивает вероятность реализации отдельными узлами или их группами нештатных функций, что может привести к формированию альтернативной ЦБ. Подобный подход приводит к необходимости совершенствования математического обеспечения DLT ЦБ систем для реализации различных алгоритмов ВИС.

Таким образом, в настоящее время актуальной является задача разработки дополнительных средств математического и программного обеспечения систем с распределенным реестром на основе цепочки блоков, обеспечивающих поддержку различных алгоритмов ВИС, возможности объединения узлов в группы и формирования на их базе стратегии поведения, включаю-

щей нештатные функции: формирование ответвления обрабатываемых данных и атаку временной блокировки с целью повышения стабильности их работы.

Работа выполнена в ФГБОУ ВО «Воронежский государственный университет» в рамках одного из основных научных направлений «Вычислительные комплексы и проблемно-ориентированные системы управления».

Цель и задачи исследования. Цель работы заключается в разработке специального математического и программного обеспечения систем с распределенным реестром на основе цепочки блоков, учитывающего особенности реализации алгоритмов взаимного информационного согласования, возможность объединения отдельных узлов в группы и реализацию на их базе альтернативных вариантов стратегий поведения на основе разработки соответствующих моделей и алгоритмов, обеспечивающих повышение стабильности их работы.

Для достижения данной цели в диссертационной работе необходимо решить следующие задачи:

- провести исследование существующих подходов к управлению системами с распределенным реестром на основе цепочки блоков при достижении их узлами взаимного информационного согласования;
- осуществить формализацию процесса функционирования узла системы с распределенным реестром на основе цепочки блоков в виде конечно-автоматной модели, обеспечивающей возможность моделирования вариативности стратегии его поведения;
- разработать математическую модель процесса достижения взаимного информационного согласования в системе с распределенным реестром на основе цепочки блоков в условиях объединения отдельных узлов в группы и выбора на их основе различных вариантов стратегий поведения;
- разработать алгоритм функционирования системы с распределенным реестром на основе цепочки блоков, основанный на реализации математической модели процесса достижения взаимного информационного согласования;
- осуществить реализацию элементов программного обеспечения процесса достижения взаимного информационного согласования для систем с распределенным реестром на основе цепочки блоков.

Объект исследования: система с распределенным реестром на основе цепочки блоков.

Предмет исследования: средства математического и программного обеспечения распределенной обработки данных в условиях решения задачи достижения взаимного информационного согласования в системах с распределенным реестром на основе цепочки блоков для обеспечения возможности объединений узлов в группы и реализации на их основе различных вариантов стратегий поведения.

Методы исследования. При решении поставленных в диссертации задач использовались методы теории системного анализа, математического моделирования, теории вероятностей и математической статистики, теории

автоматов, теории коллективного поведения автоматов.

Тематика работы соответствует следующим пунктам паспорта специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»: п.3 «Модели, методы, алгоритмы, языки и программные инструменты для организации взаимодействия программ и программных систем»; п.9 «Модели, методы, алгоритмы и программная инфраструктура для организации глобально распределенной обработки данных».

Научная новизна. В работе получены следующие результаты, отличающиеся научной новизной:

- автоматная модель процесса функционирования узла системы с распределенным реестром на основе цепочки блоков, отличающаяся представлением узла конечным автоматом с переменной структурой с возможностью реализации им нештатных функций;

- математическая модель процесса достижения взаимного информационного согласования системы с распределенным реестром на основе цепочки блоков, отличающаяся её представлением в формате коллектива конечных автоматов с возможностью создания на их основе объединений (пулов) и обеспечивающая получение количественной оценки коэффициента централизации системы;

- алгоритм функционирования системы с распределенным реестром на основе цепочки блоков, отличающийся возможностью корректировки числа операций, необходимых для генерации блока в зависимости от вариантов стратегий поведения узлов и коэффициента централизации системы, и обеспечивающий заданное среднее значение времени задержки генерации блоков;

- структурная модель взаимодействия программных модулей системы управления работой системы с распределенным реестром на основе цепочки блоков, отличающаяся учетом особенностей реализации алгоритмов взаимного информационного согласия конкретных систем распределенного реестра и обеспечивающая получение значения количественной оценки уровня стабильности функционирования системы.

Положения, выносимые на защиту:

1. Автоматная модель процесса функционирования узла системы с распределенным реестром на основе цепочки блоков обеспечивает получение зависимости очередности смены вариантов стратегии поведения узла от условий состояния среды, с которой он взаимодействует на основе построения матриц состояний.

2. Математическая модель процесса достижения взаимного информационного согласования узлами системы с распределенным реестром на основе цепочки блоков позволяет получить значение количественной оценки коэффициента централизации системы путем определения ресурсных мощностей системы и каждого отдельного узла.

3. Алгоритм функционирования системы с распределенным реестром на основе цепочки блоков обеспечивает среднее значение времени задержки

генерации блока путем корректировки числа операций, необходимых для решения блока.

4. Структурная модель взаимодействия программных модулей системы управления работой систем с распределенным реестром на основе цепочки блоков обеспечивает получение значения оценки стабильности функционирования системы с учетом факторов, влияющих на вероятность формирования альтернативных цепочек блоков.

Практическая значимость. Программная реализация разработанных моделей и алгоритмов обеспечивает дальнейшее совершенствование средств математического обеспечения систем с распределенным реестром на основе цепочки блоков путем получения значения оценки стабильности их функционирования при решении задачи достижения взаимного информационного согласования для условий объединения отдельных узлов в группы и реализации на их основе различных вариантов стратегий поведения. На элементы программных средств получено свидетельство о государственной регистрации в реестре Федеральной службы по интеллектуальной собственности.

Реализация и внедрение результатов работы

Основные положения и результаты диссертационной работы реализованы в виде специального программного модуля и нашли практическое применение в работе ООО «Инженерный центр «Интегра» для совершенствования программного обеспечения систем управления системой распределенного реестра, входящих в состав защищенных АИС. Результаты внедрены в учебный процесс Академии ФСО России (г. Орел).

Апробация результатов диссертационного исследования. Основные положения диссертационной работы докладывались и обсуждались на следующих конференциях: X Всероссийская межведомственная научная конференция «Актуальные направления развития систем охраны, специальной связи и информации для нужд органов государственной власти Российской Федерации», Академии ФСО России (Орел, 2017), XXI и XXIV International Open Science Conference «Modern informatization problems in economics and safety» (Yelm, WA, USA, 2016, 2019), International Siberian Conference on Control and Communications (Tomsk, 2019).

Публикации. По результатам диссертационного исследования опубликовано 10 печатных работ, в т.ч. 3 статьи в изданиях, рекомендованных ВАК РФ, свидетельство о государственной регистрации программы, а также статья в журнале, индексируемом в международной базе цитирования Scopus. В работах, опубликованных в соавторстве и приведенных в автореферате, лично автором получены следующие результаты: [2] – алгоритмы достижения взаимного информационного согласия в системах с распределенным реестром на основе цепочки блоков; [3, 4] – модели узла на основе цепочки блоков при реализации им нештатных функций; [5] – подсистема взаимодействия программных модулей системы управления работой систем с распределенным реестром; [6] - получение оценки коэффициента централизации системы; [8, 10] - теоретико-множественное описание структуры узлов DLT ЦБ системы.

Достоверность результатов обусловлена корректным использованием теоретических методов исследования и подтверждена результатами вычислительных экспериментов и внедрения.

Структура и объем работы. Диссертация состоит из введения, пяти глав, заключения и списка литературы. Работа изложена на 120 страницах машинописного текста, включает 28 рисунков, 2 таблицы. Список литературы включает 126 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность диссертационной работы, сформулированы цель и задачи исследования, представлены основные научные результаты, а также приведены сведения об апробации и внедрении работы.

В первой главе проведено исследование существующих подходов к управлению DLT-системами при достижении взаимного информационного согласования между их узлами.

Проведен анализ свойств DLT-систем: параллельность выполнения процессов, отсутствие глобальных часов, устойчивость к отказам, асинхронность передачи сообщений. Сформулировано определение взаимного информационного согласования, рассмотрены условия достижения взаимного информационного согласования между узлами DLT-системы. На рис. 1 представлена обобщенная архитектура сети рассматриваемых DLT-систем.

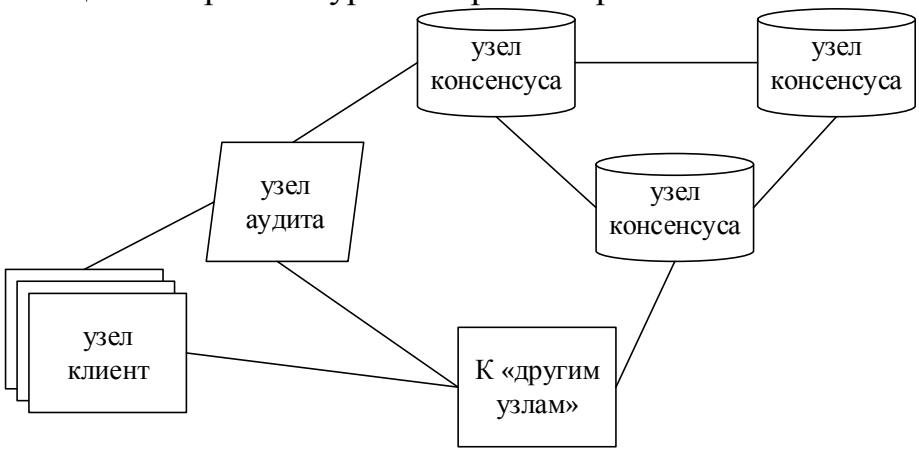


Рис. 1. Обобщенная архитектура сети DLT-систем

Рассмотрена проблема невозможности достижения ВИС между детерминированными асинхронными процессами в фиксированное время с одним неработающим процессом (проблема FLP), а также подходы к ее решению: синхронизация или использование недетерминизма. Рассмотрена устойчивость DLT-систем к сбоям и проведена классификация нарушений в работе узлов системы при достижении взаимного информационного согласования: выход из строя (сбой) работы узла, реализация нештатных функций (Византийская атака, атака Сивиллы, атаки временной задержки).

Проведено исследование существующих протоколов достижения взаимного информационного согласования между узлами DLT-системы, направленных на решение FLP-проблемы методом синхронизации и использования недетерминизма (рассмотрены DLT-системы на основе ЦБ) в условиях

сбоев при работе узлов системы и реализации нештатных функций, выделены существующие достоинства и недостатки данных решений.

Проведен анализ структуры DLT-системы на основе ЦБ при достижении взаимного информационного согласования между ее узлами, рассмотрены теоретические принципы, направленные на решение проблем сбоев и реализации нештатных функций узлами системы. Определены условия и сделан вывод о возможности реализации атак временного блокирования и формирования ответвлений обрабатываемых данных.

Проведен анализ существующих моделей peer-to-peer систем, основывающихся на алгоритмах достижения взаимного информационного согласования Накамото и GHOST.

Таким образом, проведено исследование существующих подходов к управлению DLT-системами при достижении взаимного информационного согласования между их узлами. На основании проведенного анализа сформулированы цель и задачи диссертационного исследования.

Вторая глава посвящена разработке автоматной модели процесса функционирования узла DLT-системы на основе цепочки блоков.

В реальных DLT ЦБ системах для мотивации узлов выполнять алгоритм ВИС чаще всего используется механизм поощрения за проделанную работу. Каждый узел стремится к увеличению доходности выполнения алгоритма ВИС, используя при этом различные варианты стратегии поведения и их комбинации, включая реализацию нештатных функций. При этом, если каждый узел системы будет действовать только в своих интересах и не будет стремиться поддерживать работоспособность всей системы – согласованность данных, то его доход станет равным нулю, т.к. остальные узлы не будут принимать его ЦБ.

Для формального описания процесса функционирования m-го узла DLT ЦБ системы выбрана модель конечного автомата с переменной структурой и линейной тактикой, функционирующего в среде E, представляющей собой множество узлов $A = \{a_1, a_2, \ldots, a_k\}$, $a_m \notin A$ DLT ЦБ системы, участвующих в выполнении алгоритма ВИС. В общем случае структура узла DLT ЦБ системы представлена на рис. 2.

Устойчивые состояния μ_j^i, в которых находится автомат a_m, объединяются во множество $B = \{b_1, b_2, ..., b_l\}$, именуемое «дерево», которое состоит из подмножеств b_l, именуемых «ветвь». Назовем ветви b_l, дерева $B = \{b_1, b_2, ..., b_l\}$ вариантами стратегии поведения узла при выполнении алгоритма ВИС. Смена состояний μ_j^i автомата в моменты времени t_n определяется выражением (1):

$$\mu_j^i(t_{n+1}) = \Phi[\mu_j^i(t_n), X(t_{n+1})], \quad (1)$$

где $X(t_{n+1})$ – реакция среды в момент времени t_{n+1}, $\Phi[\mu_j^i(t_n), X(t_{n+1})]$ – функция перехода, определяющая смену состояний автомата под воздействием входного сигнала – реакции среды. Разделим множество реакций среды $X(t_n)$ на

подмножества: $X(t_n)[+1]$ – класс благоприятных реакций (смена состояний μ_j^i автомата на рис. 2 обозначена сплошной линией), $X(t_n)[-1]$ – класс неблагоприятных реакций (смена состояний μ_j^i на рис. 2 обозначена пунктиром).

Зададим функцию перехода $\Phi[\mu_j^i(t_n), X(t_{n+1})]$ системой двух матриц состояний $\| a_{ij}(X(t)) \|$ $(i, j = 1,2,...,v)$, по числу классов реакций среды $X(t_n)[+1]$ и $X(t_n)[-1]$. Каждый элемент матрицы определяет вероятность перехода автомата из одного состояния μ_j^i в другое. При этом,

$$0 \le a_{ij}(X(t_n)) \le 1, \tag{2}$$

$$\sum_j a_{ij}(X(t_n)) = 1. \tag{3}$$

Определим зависимость выходного сигнала $Y(t_n)$ от устойчивого состояния μ_j^i, в котором находится автомат в момент времени t_n:

$$Y(t_n) = F[\mu_j^i(t_n)]. \tag{4}$$

Для определения оптимальной глубины памяти q_{opt} (числа устойчивых состояний в каждой ветви) автоматов с переменной структурой необходимо производить имитационные эксперименты. В связи с тем, что для каждого алгоритма ВИС конкретной DLT ЦБ системы q_{opt} будет принимать различные значения, то для обобщенной DLT ЦБ системы с абстрактным алгоритмом ВИС значение q_{opt} зададим равным 1. Согласно рассмотренным в главе 1 вариантам стратегии поведения узла DLT ЦБ системы при выполнении алгоритма достижения ВИС определим число ветвей автомата, равным четырем (на рис. 3 представлена автоматная модель m-го узла DLT ЦБ системы).

Здесь ветвь b_1 – выполнение алгоритма ВИС с вероятностью p непреднамеренного сбоя, ветвь b_2 – попытка формирования ответвления обрабатываемых данных, ветвь b_3 – публикация найденного блока, b_4 – попытка реализации атаки временного блокирования. Ветви дерева B будут иметь по одному устойчивому состоянию, определяющему стратегию поведения автомата, за исключением b_4, т.к. для успешной реализация атаки временного блокирования необходимо выполнение:

$$N_{otr} + 1 \le N_{block}, \tag{5}$$

где N_{otr} – число неблагоприятных реакций среды E, N_{block} – число блоков, найденных при выполнении стратегии временного блокирования.

Т.к. автомат имеет линейную тактику, то в ходе своего функционирования с внешней средой E он будет обучаться, и его поведение станет целесообразным за счет постоянной коррекции системы двух матриц состояний $\| a_{ij}(X(t)) \|^+$ и $\| a_{ij}(X(t)) \|^-$. В результате будут сформированы матрицы состояний и определены наиболее вероятные варианты стратегии поведения автомата в зависимости от условий среды E.

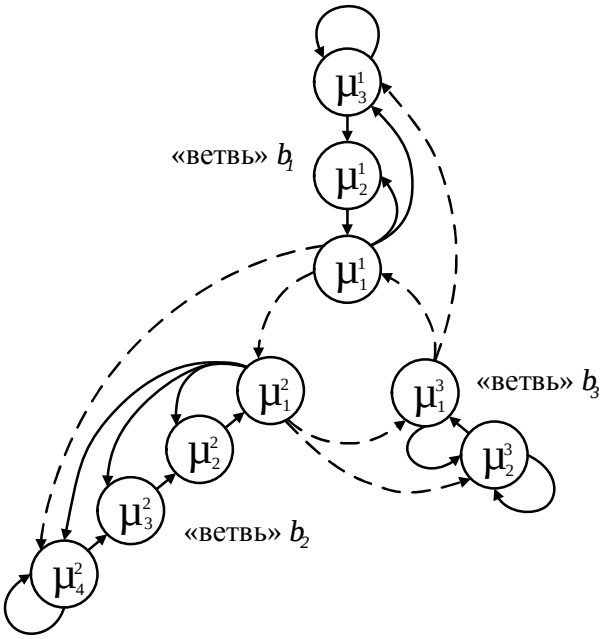


Рис. 2. Автоматная модель узла DLT ЦБ системы

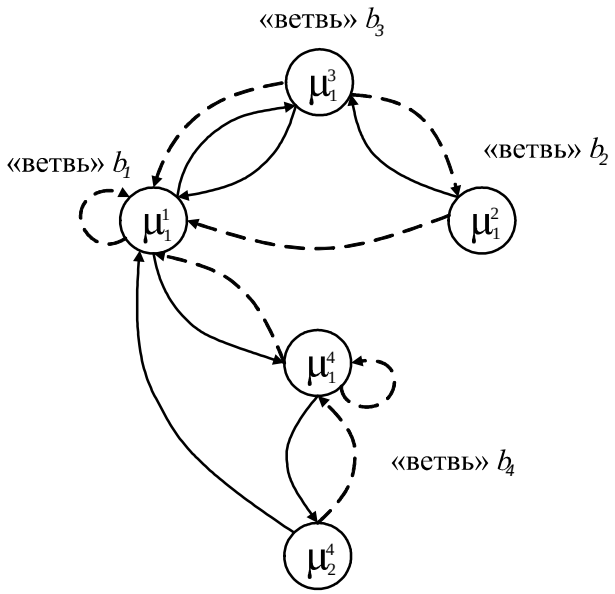


Рис. 3. Автоматная модель узла DLT ЦБ системы, учитывающая вариативность его стратегии поведения

Таким образом, разработана автоматная модель процесса функционирования узла DLT ЦБ системы, отличающаяся представлением узла конечным автоматом с переменной структурой и линейной тактикой с возможностью реализации им нештатных функций: формирования ответвления обрабатываемых данных и атаку временной блокировки и обеспечивающая получение зависимости очередности смены вариантов стратегии поведения узла от условий состояния среды, с которой он взаимодействует.

Третья глава посвящена разработке математической модели процесса достижения взаимного информационного согласования узлами DLT-системы на основе цепочки блоков.

Основываясь на автоматной модели процесса функционирования узла DLT ЦБ системы, рассмотрим процесс достижения ВИС в DLT ЦБ системе. Структурно DLT ЦБ система будет представлена децентрализованной одноранговой peer-to-peer сетью, состоящей из равноправных узлов. В DLT-системах места и время добавления или удаления узлов из сети случайны, следовательно, связи, формируемые между автоматами, также будут случайными. При этом список адресной информации автомата должен быть сформирован с учетом минимального числа исходящих соединений для различных алгоритмов достижения ВИС конкретных DLT ЦБ систем. Из этого можно сделать вывод, что среда E, в которой функционирует автомат, должна быть представлена стохастической переключаемой средой.

Рассмотрим абстрактную DLT ЦБ систему, представленную множеством A (коллективом) автоматов $a_1 - a_k$, взаимодействующих со стохастической переключаемой средой E, которая для каждого m-го автомата представлена подмножеством $A' \subset A$, таким что $a_m \notin A'$, рис. 4.

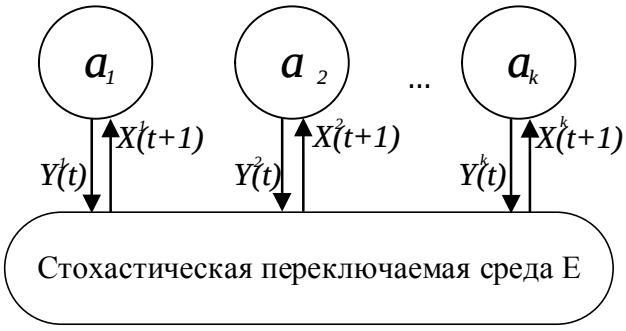


Рис. 4. Структура DLT ЦБ системы в виде коллектива автоматов

Так как различные операции, например, проверки транзакций и блоков имеют вполне определенные вычислительно-временные затраты, а добавление нового блока в ЦБ производится через усреднённо дискретные интервалы времени, примем допущение, что DLT ЦБ система функционирует в дискретном времени $t \in N_0$.

Для описания структуры протоколов достижения ВИС в DLT ЦБ системах декомпозируем алгоритм на следующие этапы: определение лидера – узла, генерирующего следующий блок, и принятие нового блока узлами.

На этапе определения лидера в алгоритмах достижения ВИС используется класс алгоритмов доказательства «Proof-of-X». Формализуем протоколы определения очередности формирования блоков в виде функции $P(t_n, A)$, где t_n – n-й интервал времени, A – множество автоматов, участвующих в алгоритме достижения ВИС. Функция $P(t_n, A)$ с некоторой вероятностью генерирует номер автомата $a_m \in A$. Вероятность $p^m_{t_n}$ генерации m-го номера автомата на интервале времени t_n определяется следующим выражением:

$$p^m_{t_n} = \frac{1}{T} * \frac{h_m}{\sum_{z=1}^{|A|} h_z}, \qquad (6)$$

где T – заданный интервал времени задержки генерации блоков, определяется требованиями безопасности конкретной реализации алгоритма ВИС, h_m – ресурсная мощность автомата a_m, $\sum_{z=1}^{|A|} h_z$ – суммарная ресурсная мощность всего множества автоматов A.

На этапе принятия нового блока узлами DLT ЦБ системы должен быть определен порядок формирования ЦБ. В ходе работы были рассмотрены наиболее распространенные протоколы ее формирования: по правилу ВИС Накамото и протоколы, основывающиеся на правиле самого «тяжелого» дерева GHOST. На рис. 5 представлен пример определения валидной ЦБ узлами DLT ЦБ системы для различных алгоритмов достижения ВИС.

Представим процесс достижения ВИС узлами DLT ЦБ системы коллективной игрой Γ автоматов. Тогда набор выходных сигналов $Y(t_n) = (Y^1(t_n), Y^2(t_n), ..., Y^{|A|}(t_n))$ в момент времени t_n, где $Y^m(t_n)$ – выходной сигнал m-го узла DLT ЦБ системы в момент времени t_n, назовем партией игры Γ. Набор $X(t_{n+1}) = (X^1(t_{n+1}), X^2(t_{n+1}), ..., X^{|A|}(t_{n+1}))$ значений входных переменных $X^m(t_{n+1})$ в момент времени t_{n+1}, отнесенных к классам $X(t_n)[+1]$ или

$X(t_n)[-1]$, назовем исходом партии $Y(t_n)$.

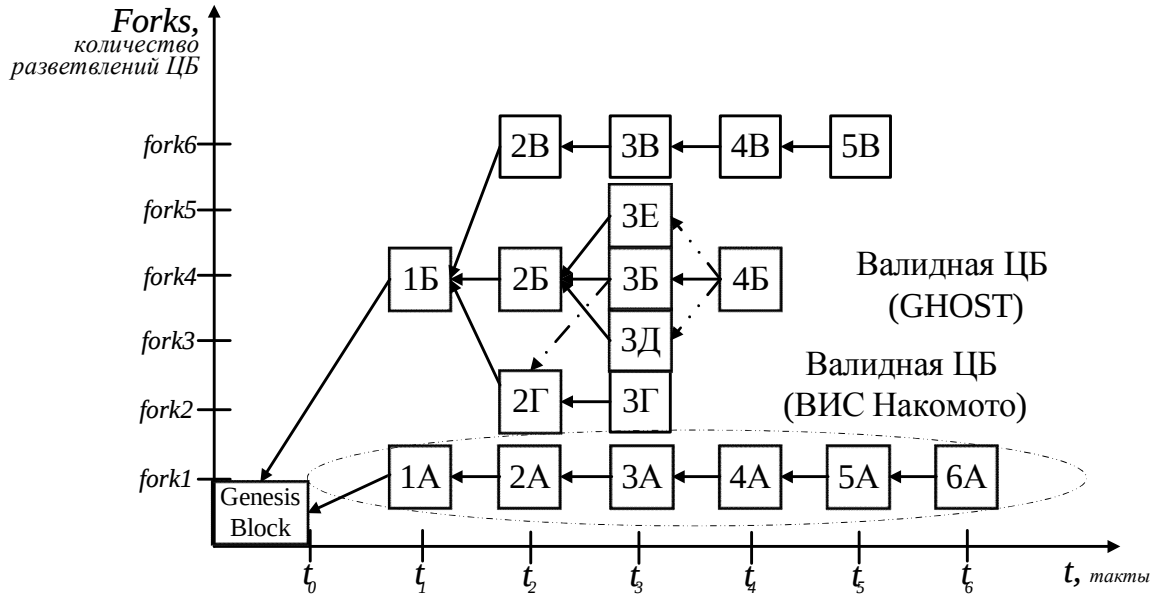


Рис. 5. Определение валидной ЦБ узлами DLT ЦБ системы в ходе достижения ВИС

Зададим игру Г вероятностями $P(Y(t_n), X(t_{n+1}))$ исхода $X(t_{n+1})$ каждой партии $Y(t_n)$ для каждого автомата из множества A. При этом

$$\sum_{z=1}^{|A|} P(Y(t_n), X^z(t_{n+1})) = 1 \qquad (7)$$

для любого $Y(t_n)$. Тогда система вероятностей $P(Y(t_n), X^z(t_{n+1}))$ будет задавать игру $|A|$ лиц.

В ходе постоянной подстройки под изменяющиеся условия каждый m-й автомат стремится к увеличению доходности выполнения алгоритма ВИС, т.е. стремится получать такие наборы $X(t_{n+1})$, чтобы входная переменная $X^m(t_{n+1})$ как можно чаще относилась к классу $X(t_n)[+1]$.

Определим математическое ожидание $M^m(t_n)$ получения наборов $X(t_{n+1})$, отнесенных к $X(t_n)[+1]$ для m-го автомата, в партии $Y(t_n)$ и зададим его формулой:

$$M^m(t_n) = \sum_{X^1(t_{n+1}),\dots X^{m-1}(t_{n+1}),X^{m+1}(t_{n+1}),\dots,X^{|A|}(t_{n+1})} [P(Y(t_n), X^1(t_{n+1}),\dots, X^{m-1}(t_{n+1}), +1, X^{m+1}(t_{n+1}),\dots X^{|A|}(t_{n+1})) -$$
$$P(Y(t_n), X^1(t_{n+1}),\dots, X^{m-1}(t_{n+1}), -1, X^{m+1}(t_{n+1}),\dots X^{|A|}(t_{n+1}))]. \qquad (8)$$

Стремление увеличить доходность выполнения алгоритма ВИС каждым отдельным узлом DLT ЦБ системы приводит к появлению эффекта групп (совместного поведения) путем структурно-параметрических модификаций, таких, например, как объединение нескольких узлов в группы (пул). Данный подход приводит к централизации и увеличению доли сгенерированных блоков определенной группой узлов, что повышает вероятность реализации отдельными узлами или их группами нештатных функций и негативно влияет на стабильность работы всей системы. На рис. 6 представлена

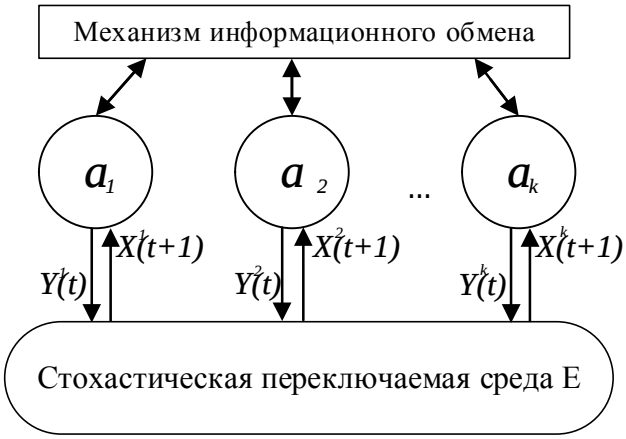


Рис. 6. Структура DLT ЦБ системы в виде коллектива автоматов с возможностью объединения в группы

структура DLT ЦБ системы, учитывающая возможность объединения отдельных узлов в группы посредством механизма информационного обмена.

Для оценки централизации системы введем показатель W, отражающий отношение максимального значения ресурсных мощностей h_z, сосредоточенных в одной группе (пуле) или узле DLT ЦБ системы, к общему значению ресурсной мощности всей системы $\sum_{z=1}^{M} h_z$, где M – число групп и отдельных узлов в системе: $W = \frac{Max(h_z)}{\sum_{z=1}^{M} h_z}$. Вероятность образования альтернативной ЦБ в результате реализации одного или нескольких вариантов стратегии нештатного функционирования узла увеличивается с ростом централизации системы.

Таким образом, в главе предложена математическая модель процесса достижения взаимного информационного согласования между узлами DLT ЦБ системы, отличающаяся представлением системы коллективом конечных автоматов с возможностью создания ими объединений (пулов) и обеспечивающая получение оценки централизации системы в условиях выбора автоматами различных вариантов стратегии поведения.

В четвертой главе представлены разработанные алгоритмы функционирования DLT-системы на основе цепочки блоков.

Исходя из представления DLT ЦБ системы, как стохастической переключаемой среды E, работающей в дискретном времени $t \in N_0$, и вариативности стратегий поведения узлов системы в ходе достижения ВИС, разработаны алгоритмы процессов функционирования DLT ЦБ системы и отдельного узла, рис. 7 и 8.

Алгоритм функционирования DLT ЦБ системы является итерационным и учитывает возможность сбоев в работе узлов, отсутствие сгенерированных блоков на интервале времени t_n, образованном заданным периодом задержки T генерации блоков.

Алгоритм поддерживает заданное значение времени задержки T между периодами генерации блоков путем корректировки числа операций необходимых для решения блока на каждом интервале времени t_n. Таким образом, алгоритм позволяет увеличить стабильность работы системы и выполнить требования безопасности конкретных алгоритмов ВИС – среднее число генерации блоков за период времени T.

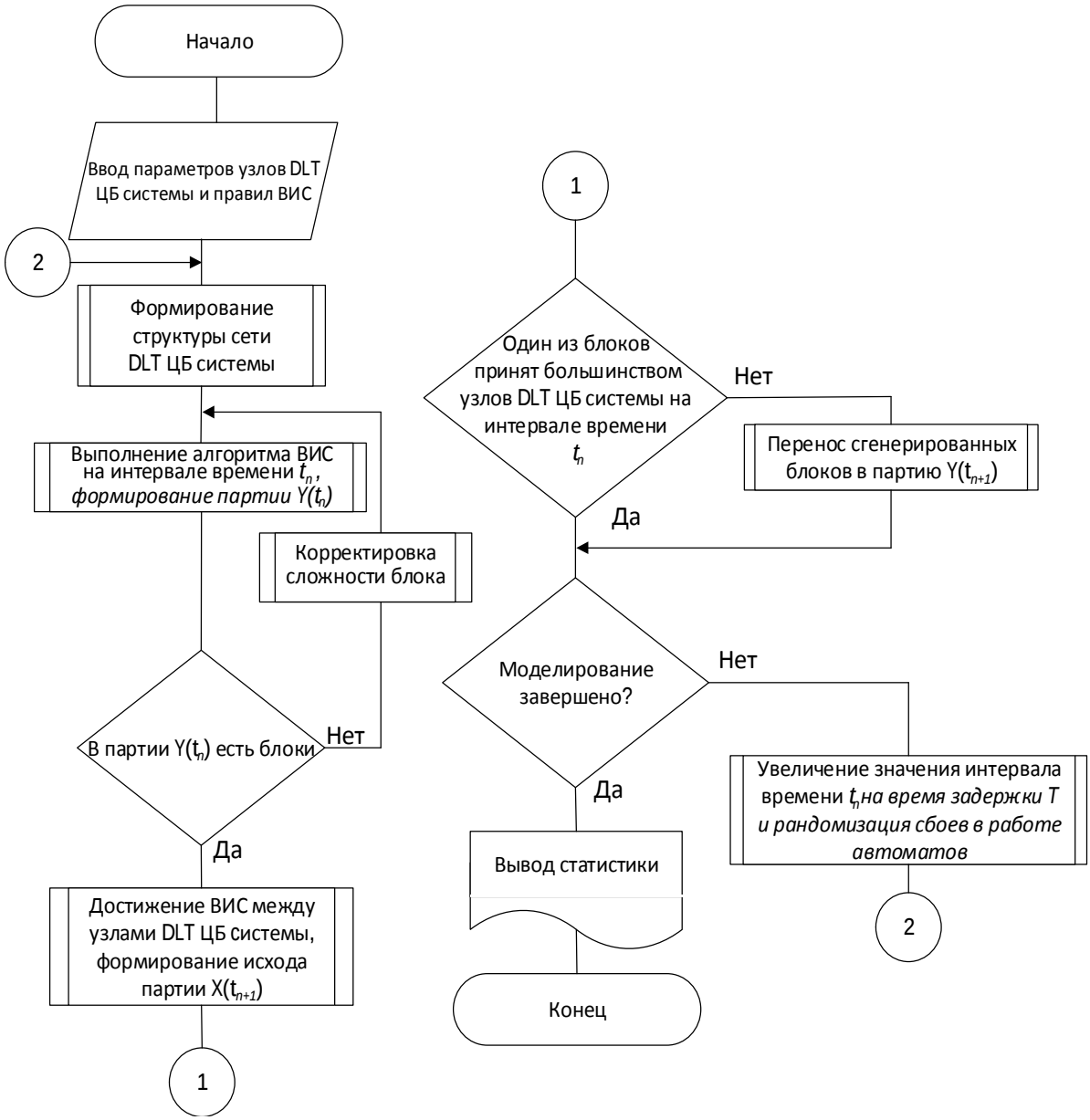


Рис. 7. Алгоритм функционирования DLT ЦБ системы

Алгоритм процесса функционирования узла DLT ЦБ системы обеспечивает формирование стратегии поведения узла. Выбор вариантов стратегии поведения осуществляется системой двух матриц состояний $\| a_{ij}(X(t_n)) \|^+$ и $\| a_{ij}(X(t_n)) \|^-$: благоприятных $X(t_n)[+1]$ и неблагоприятных $X(t_n)[-1]$ реакций среды E соответственно. В ходе игры Г автоматы обучаются и вносят изменения в элементы матриц состояний, определяющих вероятность перехода автомата из одного состояния μ_j^i в другое с учетом выполнения выражений (2) и (3). В главе представлен пример работы алгоритма функционирования DLT ЦБ системы и дано аналитическое доказательство корректности работы алгоритмов.

Таким образом, на основе предложенных в главах 2 и 3 моделей разработаны алгоритмы процесса функционирования отдельного узла и DLT ЦБ системы в ходе достижения ВИС, обеспечивающие заданное среднее значение времени задержки генерации блоков путем изменения сложности генера-

ции блока на каждом интервале времени в зависимости от выбора вариантов стратегий поведения узлов и централизации системы.

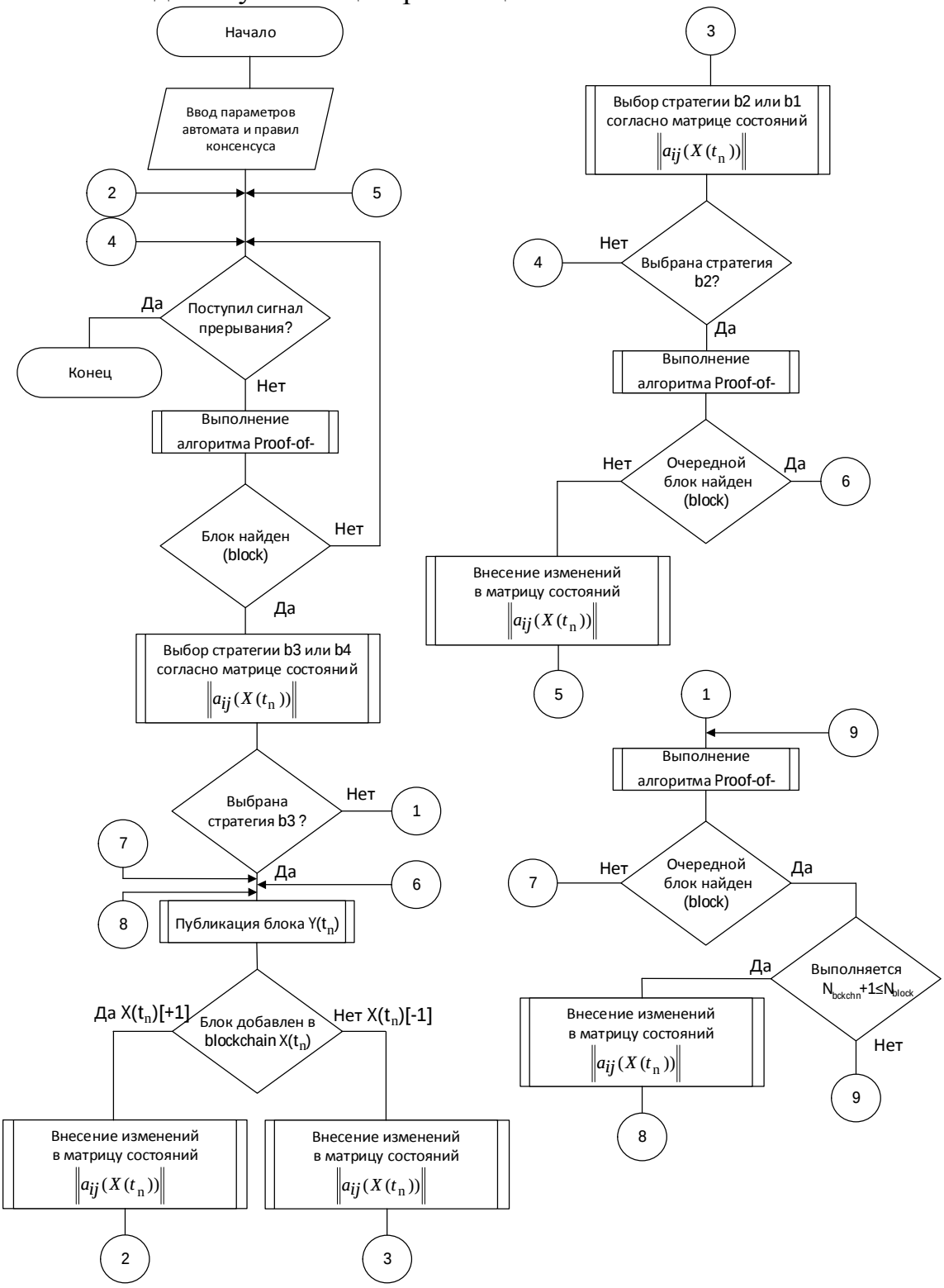


Рис. 8. Алгоритм процесса функционирования узла DLT ЦБ системы

В пятой главе предложена модульная структура программного обеспечения процесса управления системы управления работой DLT-системы на основе цепочки блоков.

При разработке программного обеспечения системы управления DLT ЦБ системой были рассмотрены такие статистические данные функциониро-

вания реальных платежных peer-to-peer систем, как: динамика изменения количества узлов в единицу времени, вероятность сбоев, зависимость числа попыток формирования fork версии ЦБ от централизации DLT-системы и т.д. Полученные данные были учтены при формировании баз данных параметров сети. Модульная структура программного обеспечения процесса управления DLT ЦБ системы представлена на рис. 9.

Декомпозиция разработанных модулей формирования параметров узлов DLT ЦБ системы и моделирования работы алгоритма ВИС представлены на рис. 10 и 11.

Учет особенностей реализации протоколов конкретных DLT ЦБ систем реализован в модуле определения валидной ЦБ (ВИС Накамото, GHOST, и т.д.) и модуле БД параметров сети путем загрузки параметров из модуля интерфейса пользователя, рис. 11. Модуль определения валидности ЦБ (ВИС Накамото, GHOST, и т.д.) позволяет использовать для определения очередности добавления блоков в ЦБ особенности реализации различных алгоритмов ВИС таких, как правила наиболее «длинной» ЦБ и наиболее «тяжелой» ЦБ.

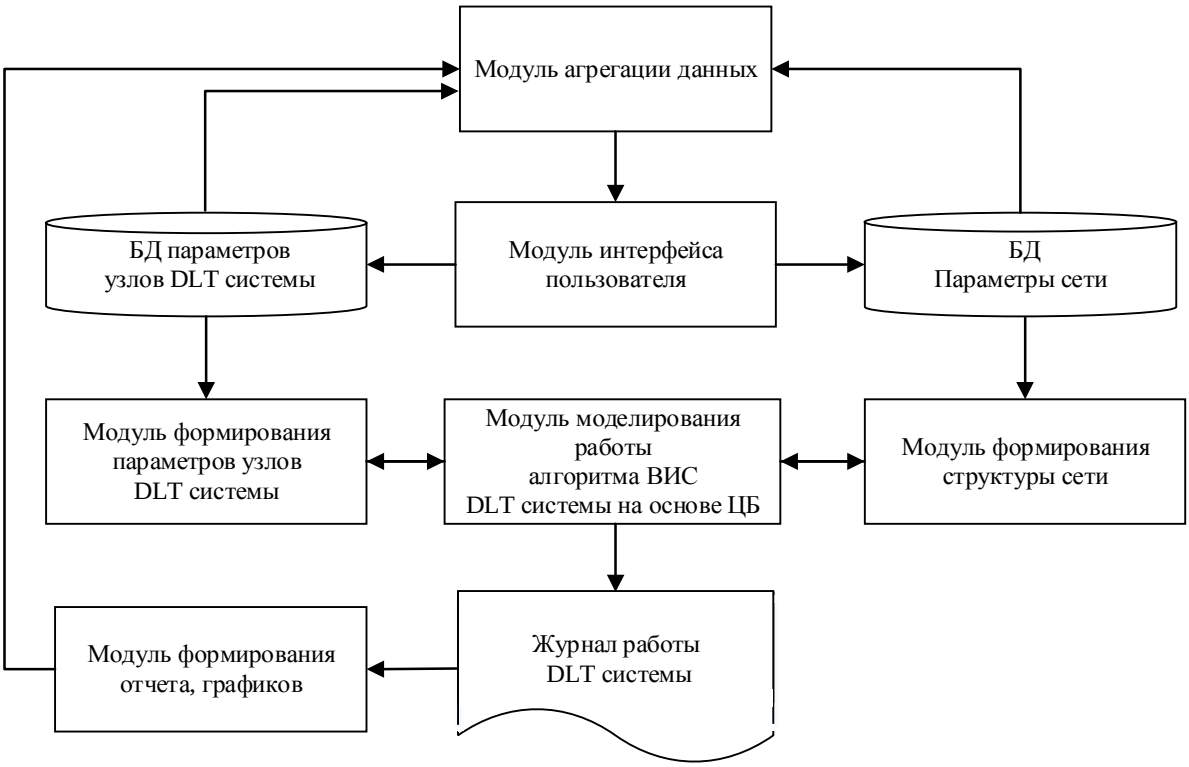


Рис. 9. Модульная структура программного обеспечения процесса управления DLT ЦБ системы

Представленные на рис. 9-11 структуры реализованы в виде программного обеспечения в интегрированной среде программирования C++ Builder на языке программирования C++. Программа создана для работы под управлением операционной системы Windows (Windows 7 и более поздние), работа под управлением других операционных систем не предусмотрена. На разработанное программное обеспечение получено свидетельство о государственной регистрации программы для ЭВМ в реестре Федеральной службы по интеллектуальной собственности.

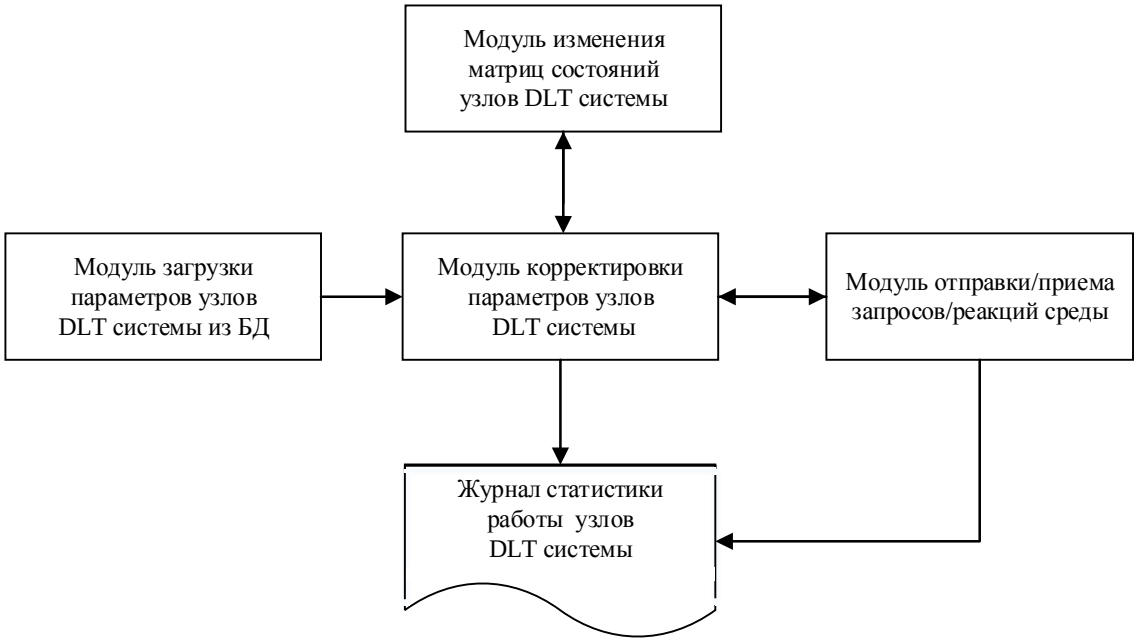


Рис. 10. Структура информационного взаимодействия в модуле формирования параметров узлов DLT ЦБ системы

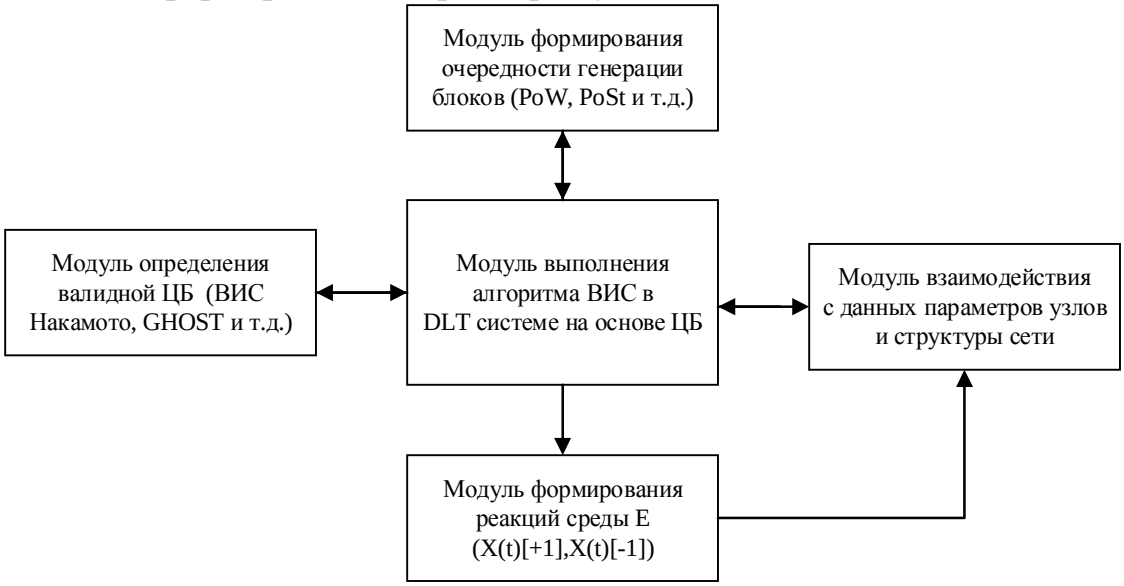


Рис. 11. Структура информационного взаимодействия в модуле моделирования работы алгоритма ВИС DLT ЦБ системы

В ходе проведения экспериментов была доказана эффективность разработанного специального программного обеспечения. Для проведения оценки эффективности использованы данные платежной peer-to-peer системы Bitcoin. В течение заданного периода (1 млрд. тактов) между 10000 узлами системы выполнялся алгоритм достижения ВИС Накамото. При этом в течение первых 100000 тактов моделирования наблюдалось значительное отклонение от показателей реальной системы из-за периода обучения конечных автоматов. При частой смене состояний среды (чаще, чем раз в 10000 тактов) моделирование также не обеспечивало удовлетворительных результатов по причине невозможности выбора автоматами оптимальной стратегии поведения. Поэтому применение разработанного специального программного обеспечения целесообразно после обучения коллектива конечных автоматов

на конкретной реализации алгоритма достижения ВИС и при относительной стационарности среды функционирования, т.е. низких значениях вероятностей добавления и удаления узлов из системы во время выполнения алгоритма ВИС.

В ходе достижения ВИС узлы системы на основании статистической информации формируют значение коэффициента централизации системы. В случае генерации двух и более блоков в течение одного периода времени, узлы на основании статистики выбирают блок, владелец которого имеет меньшее значение ресурсной мощности. Данное правило повышает стабильность системы (вероятность формирования единой ЦБ) с ростом значения ресурсной мощности узла (пула) по отношению к штатной работе алгоритма ВИС рис. 12.

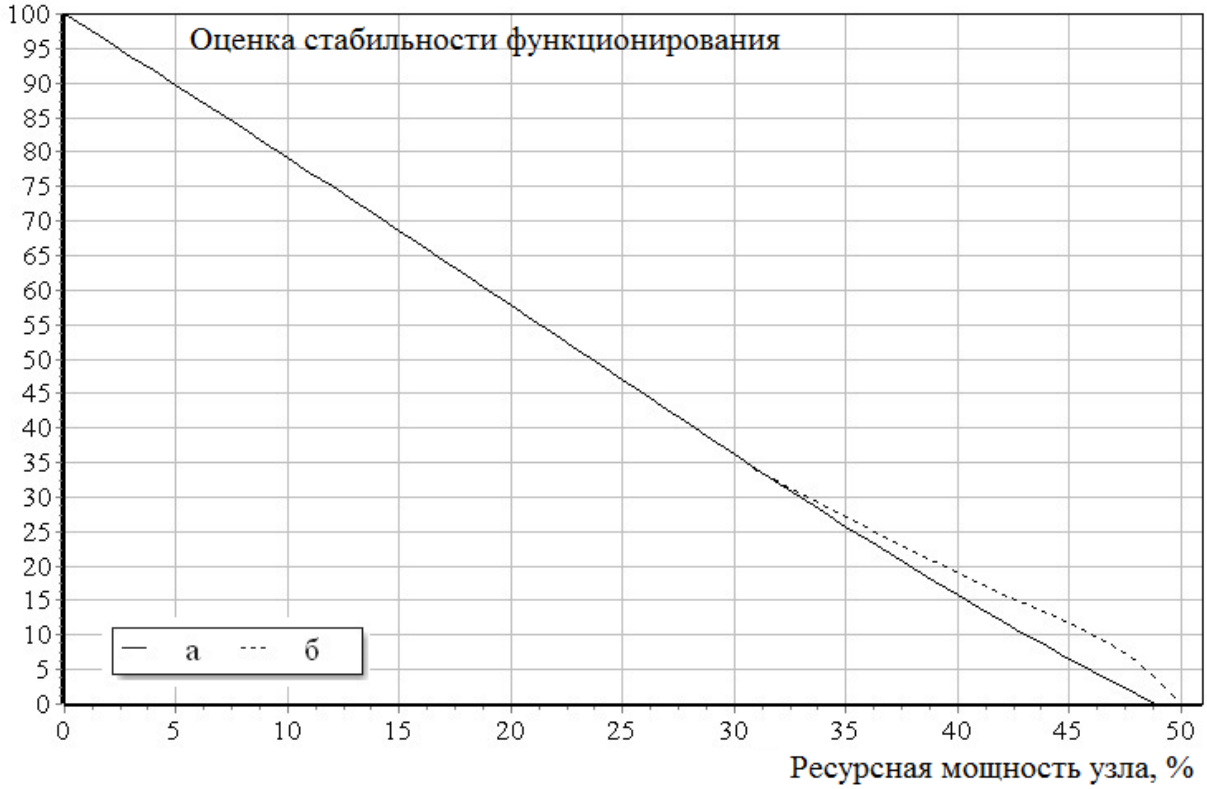


Рис. 12. Зависимость оценки стабильности функционирования системы от ресурсной мощности узла: а) штатная работа алгоритма ВИС; б) разработанный алгоритм, учитывающий нештатные функции узлов и централизацию системы

Таким образом, учет вариативности стратегии поведения узлов системы, возможности объединения их в группу и корректировка сложности блока в ходе ВИС увеличивает вероятность формирования единой ЦБ (стабильности системы) при значении ресурсной мощности в диапазоне от 33% до 50% в среднем на 4% по отношению к другим системам управления DLT ЦБ системой, не учитывающих этих факторов.

Разработанная модульная структура программного обеспечения процесса управления системы управления работой DLT ЦБ систем при ее реализации обеспечивает получение значения оценки стабильности функционирования системы с учетом факторов, влияющих на вероятность формирования

альтернативных цепочек блоков: реализация нештатных функций, централизация сети, особенности реализации алгоритма ВИС.

ЗАКЛЮЧЕНИЕ

В процессе выполнения диссертационного исследования получены следующие основные результаты:

1. Проведено исследование существующих подходов к управлению системами с распределенным реестром на основе цепочки блоков при достижении их узлами взаимного информационного согласования.

2. Формализован процесс функционирования узла системы с распределенным реестром на основе цепочки блоков в виде конечного автомата с переменной структурой, который обеспечивает получение зависимости очередности смены вариантов стратегии поведения узла от условий состояния среды, с которой он взаимодействует.

3. Разработана математическая модель процесса достижения взаимного информационного согласования системы с распределенным реестром на основе цепочки блоков, которая обеспечивает получение значения оценки коэффициента централизации системы при объединении отдельных узлов в группы.

4. Разработан алгоритм функционирования системы с распределенным реестром на основе цепочки блоков, который обеспечивает заданное среднее значение времени задержки генерации блоков в зависимости от вариантов стратегий поведения узлов и коэффициента централизации системы.

5. Реализованы элементы специального программного обеспечения управления работой системы с распределенным реестром на основе цепочки блоков, которые обеспечивают получение значения оценки стабильности функционирования системы с учетом факторов, влияющих на вероятность формирования альтернативных цепочек блоков.

6. Элементы специального программного обеспечения зарегистрированы в реестре Федеральной службы по интеллектуальной собственности.

Полученные результаты могут найти применение в сфере финансов, медицинской отрасли, логистике, государственном управлении при разработке и модернизации децентрализованных одноранговых сетей, используемых для сбора, безопасного хранения и обработки данных. Направления дальнейших исследований могут заключаться в разработке новых подходов к формированию матриц состояний узлов системы, анализу возможности реализации атак Сивиллы при использовании предложенных алгоритмов.

Основные результаты диссертации опубликованы в следующих работах:

Публикации в изданиях списка ВАК

1. Еськов С.С. Моделирование платежной системы Bitcoin на основе теории коллективного поведения автоматов// Системы управления и информационные технологии, №4(78), 2019. – С. 79-83.

2. Еськов С.С., Кравец О.Я. Алгоритмизация взаимного информационного согласия в системах с распределенным реестром на основе цепочки блоков// Моде-

лирование, оптимизация и информационные технологии, 2020, 8(2). https://moit.vivt.ru/wp-content/uploads/2020/05/EskovKravets_2_20_1.pdf.

3. Еськов С.С., Кравец О.Я. Моделирование работы узла DLT системы на основе цепочки блоков при реализации им нештатных функций в ходе достижения взаимного информационного согласия// Системы управления и информационные технологии, №2(80), 2020. – С. 67-71.

Публикации в изданиях, индексируемых в Scopus

4. Filimonov P.A., Izotova T.Y., Gorelik S.S., Eskov S.S. The question simulation of internet data exchange, according the features of functioning the hybrid content delivery networks// Journal of Physics: Conference Series, 2019. Vol. 1399 – No. 3. ISSN 1742-6596. https://iopscience.iop.org/article/10.1088/1742-6596/1399/3/033017/pdf.

Свидетельство о государственной регистрации программ

5. Лебеденко Е.В., Еськов С.С. Программа Two-Level Blockchain «TLB». – Свидетельство о государственной регистрации программы для ЭВМ № 2019616800 от 29.05.2019. М.: ФИПС, 2019.

Статьи и материалы конференций

6. Eskov S.S., Lebedenko E.V. Approaches to access limitation to the automated system for organizational units evaluation// Modern informatization problems in economics and safety: Proceedings of the XXI-th International Open Science Conference. – Yelm, WA, USA: Science Book Publishing House, 2016. – P.35-39.

7. Eskov S.S. Approaches to improving efficiency transaction processing in the distributed ledger systems based on blockchain technology// Modern informatization problems in economics and safety: Proceedings of the XXIV-th International Open Science Conference. – Yelm, WA, USA: Science Book Publishing House, 2019. – P.49-53.

8. Еськов С.С., Лебеденко Е.В., Чемодуров М.В. Исследование методов коллективного поведения автоматов при моделировании систем распределенного реестра на базе технологии блокчейн// Информационные технологии моделирования и управления, №4(118), 2019. – С. 278-285.

9. Еськов С.С. Подходы к повышению оперативности обработки транзакций в системах распределенного реестра на базе технологии блокчейн// 2019 International Siberian Conference on Control and Communications: IEEE Catalog Number CFP19794-CDR. ISBN 978-1-5386-5141-4, 2019.

10. Еськов С.С., Кравец О.Я. Проблемы и решения взаимного информационного согласования в системах распределенного реестра// Информационные технологии моделирования и управления, №2(120), 2020. – С. 138-153.

Подписано в печать 07.07.2020.
Формат 60x84/16. Бумага для множительных аппаратов.
Усл. печ. л. 1,0. Тираж 80 экз. Заказ №
ФГБОУ ВО «Воронежский государственный технический университет»
394026 Воронеж, Московский просп., 14