Научная статья
УДК 004.75
DOI:10.31854/1813-324X-2022-8-4-65-73

Модели применения блокчейн в государственных информационных системах

Василий Сергеевич Елагин, elagin.vas@gmail.com

Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация: *Целью статьи является исследование и моделирование отдельных аспектов (методов, алгоритмов обработки заявлений) внедрения технологии блокчейн в отдельные элементы государственных информационных систем. Для достижения поставленной цели в статье последовательно рассмотрены следующие вопросы: анализ технических возможностей блокчейн, анализ алгоритмов обработки заявлений на государственном портале, исследование технологической особенности развертывания сети блокчейн для повышения эффективности предоставления услуг, разработка аналитических соотношений для исследования зависимости времени обработки, разработка имитационной модели для исследования вероятностных характеристик времени обработки. В статье предложена модель применения технологии блокчейн в государственных информационных системах, например, на портале государственных услуг, с учетом большого числа органов власти, участвующих в процессе.*

Ключевые слова: *блокчейн, государственные информационные системы, портал госуслуг, аутентификация услуг, сетевые харакетристики*

Ссылка для цитирования: Елагин В.С. Модели применения блокчейн в государственных информационных системах // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 65–73. DOI:10.31854/1813-324X-2022-8-4-65-73

Models of Blockchain Application in Government Information Systems

Vasiliy Elagin, elagin.vas@gmail.com

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

Abstract: *The purpose of the article is to study and model certain aspects (methods, algorithms for processing applications) of introducing blockchain technology into individual elements of state information systems. To achieve this goal, the following issues are sequentially considered in the article: analysis of the technical capabilities of blockchain, analysis of algorithms for processing applications on the state portal, study of the technological features of deploying a blockchain network to improve the efficiency of service provision, development of analytical relationships for studying the dependence of processing time, development of a simulation model for research processing time probabilistic characteristics. The article proposes a model for the application of blockchain technology in public information systems, for example, on the portal of public services, taking into account the large number of authorities involved in the process.*

Keywords: *blockchain, government information systems, public services portal, service authentication, network characteristics*

For citation: Elagin V. Models of Blockchain Application in Government Information Systems. *Proc. of Telecom. Universities.* 2022;8(4):65–73. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-65-73

Введение

Технология Blockchain (*акр. от англ*. Blockchain – цепь из блоков; далее по тексту – блокчейн) – это сеть с распределенной базой данных (реестром). Информация в технологии блокчейн не хранится на одном узле, а дублируется на территориально распределенные аппаратно-программные комплексы по всему миру. Данную сеть из равнозначных компьютеров принято называть одноранговой или P2P-сетью (*от англ*. Peer-to-Peer – равный к равному). На каждом из таких компьютеров хранится полная версия блокчейн (полная цепочка блоков) и, при добавлении блока, информация на всех компьютерах обновляется. Это гарантирует, что информация общедоступна, не может быть подделана или удалена, а совершенные действия открыты к просмотру любым пользователям.

Параллельно происходит активное развитие информационных сервисов для государственных нужд. Государственная информационная система о государственных и муниципальных платежах (ГИС ГМП) – система, предназначенная для хранения и обмена информацией о платежах между администраторами доходов, организациями по приему платежей и гражданами, созданная в соответствии с Федеральным законом Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Система «Управление» представляет собой комплекс информационных систем и информационных ресурсов, включающий центральную информационную систему, ведомственные информационные системы, информационные ресурсы которых предназначены для принятия управленческих решений в сфере государственного управления, а также информационные ресурсы иных информационных систем (в том числе региональных). Доступ к открытой части государственной информационной системы «Управление» осуществляется по адресу: http://gasu.roskazna.ru.

Единый портал государственных и муниципальных услуг (или Госуслуги) – это федеральная государственная информационная система. Она обеспечивает гражданам, предпринимателям и юридическим лицам доступ к сведениям о государственных и муниципальных учреждениях и оказываемых ими электронных услугах. Требования к ней перечислены в Постановлении Правительства Российской Федерации от 24 октября 2011 г. № 861 и других нормативно-правовых актах. Оператором портала назначено Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации[1].

Стремительный рост развития и увеличение сфер применения трафика технологии блокчейн заставляет задуматься о применении концепции технологии в ГИС, например, такой системы как портал государственных услуг. Технические возможности, которые открывает блокчейн позволят повысить эффективность предоставления услуг в государственных информационных системах, однако, первоначально необходимо оценить потенциальное воздействие технологии на сеть, аппаратные и программные ресурсы, для избежания негативных последствий. Поэтому целью статьи является исследование и моделирование отдельных аспектов (методов, алгоритмов обработки заявлений) внедрения технологии блокчейн в государственные информационные системы.

Технологические особенности блокчейн

В контексте поставленной цели следует выделить основные технологические преимущества блокчейн:

– децентрализация и распределенность;
– безопасность и защищенность;
– открытость и прозрачность;
– неизменность уже записанного.

Децентрализация и распределенность. Информация о транзакциях хранится на тысячах компьютерах, находящихся под владением майнеров, которые отвечают за проверку и добавление блокчейн в виде новых блоков. Майнеров может быть тысячи в одной сети, и над ними нет централизированного управления. Таким образом вся информация распределена на сети, а вероятность того, что все компьютеры выйдут из строя, ничтожно мала.

Безопасность и защищенность. Попытки взломать один из блоков и изменить информацию в нем не имеет смысла, поскольку изменять придется все блоки, а также копии базы на всех компьютерах, а для этого нужны колоссальные вычислительные мощности. К тому же препятствием к фальсификации является и мощный алгоритм шифрования с использованием хеш-функций, а также цифровой подписи. Чтобы изменить цифровую подпись на одном из блоков, нужно изменить цифровые подписи на последующих за ним блоках. Таким образом взломщик чисто физически не сможет поменять подписи на всех последующих блоках, так как их тысячи, и скорость создания новых блоков выше, чем скорость, с которой взломщик будет менять подписи на старых блоках.

Открытость и прозрачность. Вся база находится в публичном доступе, а потому посмотреть данные того или иного блока может любой желающий.

Неизменность уже записанного. Каждый вновь созданный блок в блокчейн содержит в зашифрованном виде данные о предыдущих блоках (хеш-сумма предыдущих блоков). Таким образом, технология блокчейн изначально предопределяет невозможность добавления фальшивого блока или изъятие существующего, поскольку это приведет к изменениям во всей системе. При удалении блока система точно также отреагирует на изменение глобальной структуры. Как результат – мошенничество, попытки несанкционированного вмешательства или то же пиратство практически исключены.

Однако необходимо отметить и недостатки блокчейн технологии, оказывающие существенное влияние на ее приложения, а именно:

– низкая масштабируемость (с увеличением количества пользователей происходит значительный рост размеров блока);

– мошенничество и ошибки (невозможно обратить ошибочные действия);

– низкая скорость обработки транзакций (медленный процесс обработки, особенно в сравнении с сетевой задержкой при использовании его в синхронных сервисах реального времени);

– отсутствие единого стандарта;

– ограничение объема данных, добавляемых в блок.

Архитектура портала Госуслуг

По мере расширения цифровой экономики неизбежно увеличивается потребность в цифровой трансформации государственных услуг. Формат цифрового сервиса не только удобен для потребителя, но одновременно с этим цифровой сервис позволяет предприятию автоматизировать и оптимизировать процессы и отдельные операции, лежащие в основе его предоставления [2]. Предоставление персонализированных услуг гражданам, предприятиям и некоммерческим организациям потребует фундаментальных изменений в работе государственных учреждений путем интеграции процессов, объединения пользовательских данных и предоставления к ним доступа, а также интеграции как существующих, так и разрабатываемых информационных систем [3].

Эффективная информационная архитектура портала позволяет быстро, легко и интуитивно находить на нем интересующий контент. Это дает возможность избежать увеличения времени предоставления услуги при личном посещении государственных органов, предоставляющих услугу, или нахождение в очереди в единых МФЦ России.

Общая архитектура портала представлена на рисунке 1. Она позволяет увеличивать существующий функционал, а также добавлять к проекту новых участников для распараллеливания процесса разработки и совершенствования.

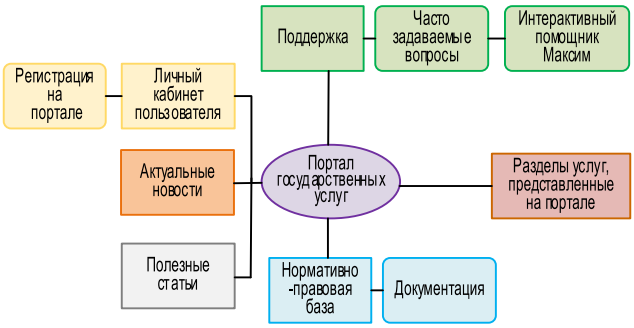

Рис. 1. Общая архитектура портала

Fig. 1. General Architecture of the Public Services Portal

Система межведомственного электронного взаимодействия

Единая система межведомственного электронного взаимодействия (СМЭВ) представляет собой федеральную ГИС, включающую информационные базы данных, в том числе содержащие сведения об используемых органами и организациями программных и технических средствах, гарантирующих возможность доступа посредством информационно-технического взаимодействия к их информационным системам, о программных и технических средствах, поддерживающих единый документированный способ взаимообмена информационных систем органов и организаций посредством технологии очередей электронных сообщений, обеспечивающей взаимодействие программ в асинхронном режиме, не требующим установки между ними прямой связи и гарантирующим получение передаваемых электронных сообщений, а также сведения об истории движения в системе взаимодействия электронных сообщений [4], и еще целый ряд контекстных сведений.

Обмениваться данными через СМЭВ органы власти должны в двух направлениях. Если заявитель запрашивает федеральную услугу, то территориальное подразделение федерального органа власти в случае необходимости должно иметь возможность получить сведения из регионального органа и (или) органа местного самоуправления. В случае, если заявитель обращается за региональной или муниципальной услугой, то чиновники должны суметь получить сведения в федеральном органе.

Общая схема работы сервиса представлена на рисунке 2. Сотрудник ведомства направляет запрос к сервису через СМЭВ. Сервис сохраняет поступивший запрос с указанием ведомства и его регистрирует. Далее сервис обращается к системе «Гостехнадзор Эксперт» для получения сведений. Затем система Гостехнадзора обрабатывает сам запрос и отдает результаты обработки на сервис СМЭВ, откуда отправляется ответ сотруднику ведомства – инициатору запроса.

Рис. 2. Общая схема работы СМЭВ

Fig. 2. Algorithm of Operation of the System of Interdepartmental Electronic Interaction

СМЭВ состоит из сети защищенных каналов связи между узлами, расположенными в центрах обработки данных.

Участники СМЭВ являются поставщиками и потребителями сведений:

– каждый поставщик публикует и регистрирует в СМЭВ свой электронный сервис, который предназначен для обработки запросов и выдачи сведений;

– каждый потребитель получает доступ к опубликованным сервисам в СМЭВ в случае необходимости, реализует адаптер, который умеет правильно запрашивать сведения и получать ответ.

Оператором СМЭВ является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации; посредством СМЭВ интегрирует между собой многочисленные федеральные и региональные информационные системы.

Обработка заявлений на портале государственных услуг

Порядок обработки заявлений на портале в общем виде представлена на рисунке 3. Пользователь открывает портал государственных услуг, входит в личный кабинет и выбирает категорию услуги. После этого открывается страница всех услуг представленной категории. Пользователь выбирает нужную услугу, заполняет необходимые параметры и сформировывает заявление на портале. Далее это заявление проходит обработку.

Процесс приема заявлений представлен на рисунке 4. Заявление вместе с необходимыми документами передается с портала Государственных услуг на «Веб-сервис СМЭВ Гостехнадзора». Далее оно проходит этап проверки и сохраняется в ведомственную систему, затем попадает в реестр (где ведется учет всех обработанных заявлений). После этого инспектор вручную проверяет заявление и приложенные к нему документы, через систему «Гостехнадзор Эксперт» отправляет на портал новый статус заявления, дату и время приема или причину отказа. Сообщение автоматически подписывается электронной подписью органа власти. Таким образом обрабатываются все поступившие на портал заявления, в которых необходимо участие инспектора. Общую картину (архитектуру) можно увидеть на рисунке 5.

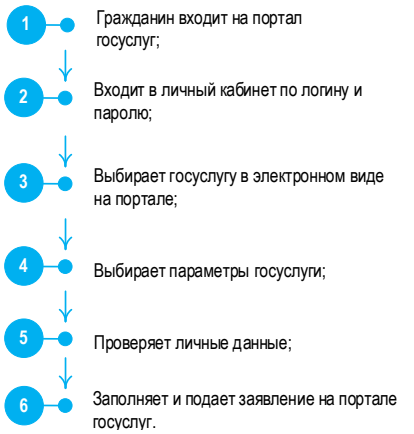

Рис. 3. Общая структура обработки заявлений на портале государственных услуг

Fig. 3. General Structure of Application Processing on the Public Services Portal

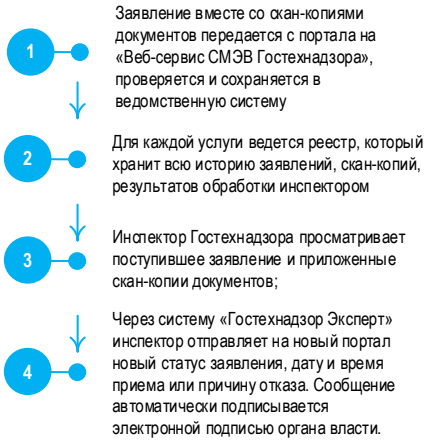

Рис. 4. Прием заявлений с портала

Fig. 4. Acceptance of Applications Via the Website

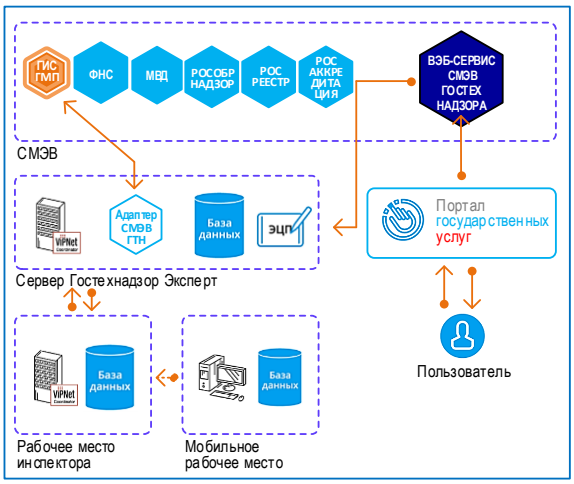

Рис. 5. Общая архитектура системы

Fig. 5. General Interaction Architecture

Алгоритм функционирования портала Госуслуги с использованием технологии блокчейн

Опираясь на вышесказанное, можно сделать вывод, что большая часть государственных услуг (а это примерно больше 170 уникальных услуг) оказывается при непосредственной работе инспектора. На диаграмме (рисунок 6) видно, что преимущественно услуги категорий «Справки и выписки», «Недвижимость/Стройка» и «Налоги/Финансы» обрабатываются инспектором. Инспектор проверяет правильность введенных данных, проверяет, есть ли у лица, подающего документы, необходимая недвижимость или льготы на оказание услуг, а также проверяет иную введенную информацию.

Рис. 6. Диаграмма распределения услуг по категориям

Fig. 6. Diagram of the Distribution of Services by Category

То есть, бóльшая часть работы по проверке производится не автоматически, а при участии инспектора. Поэтому, если будет существовать доверительная система с защитой данных, для которой известно, что данные корректны, достоверны и защищены, это значительно снизит воздействие человеческого фактора на работу всего портала.

Система на базе технологии блокчейн, которая обладает всеми параметрами для этого, может частично заменить ручную обработку инспектора на автоматическую.

В этом случае алгоритм обработки заявки выглядел бы следующим образом:

1) пользователь портала выбирает услугу;

2) пользователь заполняет необходимые данные;

3) услуга формируется и отправляется на проверку;

4) система блокчейн заполняет личные данные о пользователе, после чего они подвергаются проверке;

5) система блокчейн шифрует данные и формирует блок;

6) затем эти данные попадают на систему СМЭВ;

7) система СМЭВ сохраняет заявление с документами в ведомственную систему;

8) для заявления на оказание услуги присваивается уникальный номер;

9) система СМЭВ по тегам отправляет заявление в необходимое ведомство;

10) в ведомстве заявление расшифровывается и попадает на рабочий стол сотрудника ведомства для оказания услуг, при этом последнему не нужно проверять правильность заполненных данных, так как он может доверять предыдущей цепочке, через которую прошло заявление;

11) пользователю оказывается услуга и ее результат возвращается ему по тому же алгоритму, только в обратном направлении.

Общий алгоритм оказания услуги с использованием блокчейн-системы представлен на рисунке 7.

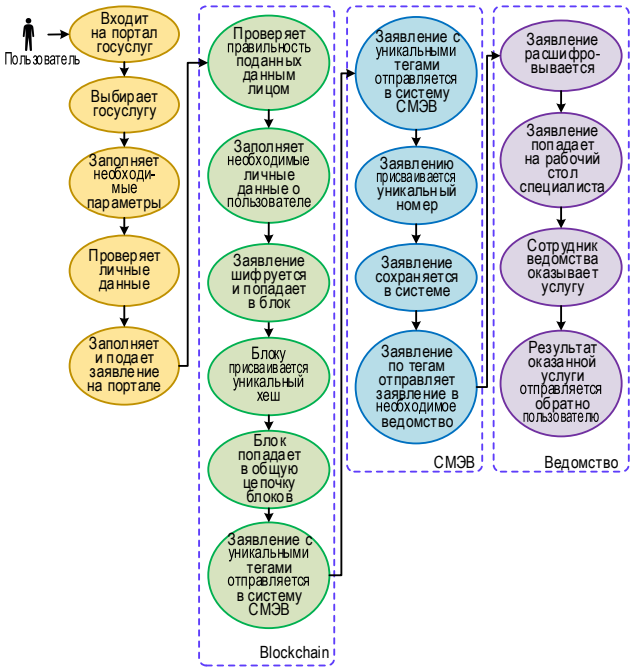

Рис. 7. Общий алгоритм оказания услуги на портале с использованием блокчейн системы

Fig. 7. A Generalized Algorithm for Providing Services on the Portal Using a Blockchain System

Таким образом, технологические решения вопроса использования блокчейн для автоматизации обработки запросов могут быть предоставлены, однако первоначально необходимо оценить вероятностно-временны́е характеристики работы портала Госуслуг при интеграции с блокчейн-системами. Технологически данная система может потребовать авторизацию услуг инспектором в нескольких государственных и региональных ведомствах для внесения в цепочку [5].

Как показано на рисунке 8, такая системная модель состоит из пяти компонентов: загрузчик (пользователь), список ведомств для авторизации данных, сервер, система блокчейн и Атор (верификатор). Пользователь загружает данные об услуге на портал; они должны быть аутентифицированы,

в нескольких ведомствах. Каждый орган использует функцию (*f*) подписей, и ему нужно только аутентифицировать свои данные – *f* (данные). Когда все ведомства успешно аутентифицируют данные, они подписывают ту их часть, за которую отвечают, и совместно создают подпись для общих данных.

Как показано на рисунке 9, информация об этом хранится в блокчейне: подписи, имя органа и дата аутентификации данных; окончательная подпись полных данных хранится в заголовке блока. Сервер отвечает за поддержание блокчейна и предоставление системных параметров для участвующих в процессе ведомств. Верификатор может запросить подпись данных на сервере и убедиться, что она действительна [6, 7].

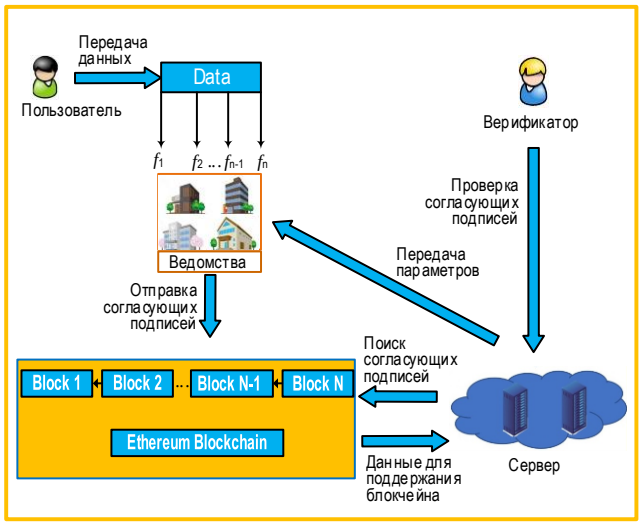

Рис. 8. Структура системной модели применения блокчейн

Fig. 8. The Structure of the System Model of Blockchain Application

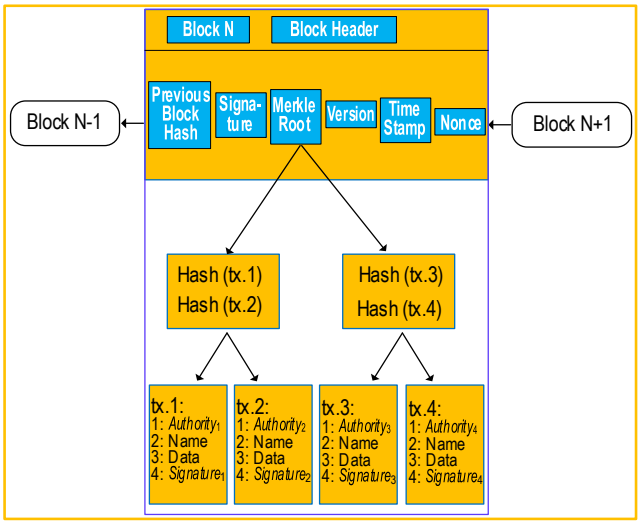

Рис. 9. Внутренняя структура блоков в предлагаемой системе

Fig. 9. The Internal Structure of the Blocks in the System

Модель системы включает в себя три различных этапа работы в смарт-контракте.

Этап 1. invokeF(f) – алгоритм компилируется сервером и может выполняться законными властями. Сервер определяет, является ли функция *f*, вызванная этим органом, легитимной по возвращаемому значению.

Этап 2. addUser(f,ct.sender) – алгоритм может выполняться только сервером. Системная модель может динамически наделять полномочия с использованием функции *f*.

Этап 3. deleteUser(f,ct.sender) – алгоритм может выполняться только сервером. Системная модель может динамически отвергать использование органом власти функции *f*.

Построение децентрализованной сети в целях обеспечения всех преимуществ технологии блокчейн возможно; достаточным будет использование существующей аппаратно-программной инфраструктуры ГИС при соответствующей доустановке и обновлении программного обеспечения.

Так как процесс внедрения децентрализованной сети блокчейн-узлов внесет дополнительный объем трафика в инфокоммуникационную сеть, оценка которого пока не проводилась в рамках других исследований, приведенные ниже соотношения призваны помочь с оценкой влияния блокчейн-узлов на загрузку сети с учетом особенностей функционирования технологии [8].

Сетевые характеристики технологии блокчейн

Процесс сетевого взаимодействия и временны́е характеристики схемы, включая проблему поиска и хранения информации, нуждаются в оценке их значений в зависимости от параметров сети.

В рамках предложенной схемы можно выделить два основных процесса, формирующих задержку: аутентификацию данных в ведомствах и работу сервера.

В исследуемой схеме каждый орган власти должен выполнять одну хэш-функцию процедуры, связанную с формирование цифровой подписи, и одну – по формированию смарт-контракта. Каждый орган власти должен вызвать один смарт-контракт, чтобы использовать функцию *f*.

Таким образом, за исключением сетевой задержки, каждому ведомству потребуется время выполнения аутентификации данных:

$$T_{Ai} = T_h + T_{Sig} + T_{SC},$$

где T_h, T_{Sig}, T_{sc} – затраты времени на выполнение одной хэш-функции, формирование цифровой подписи и одного смарт-контракта, соответственно.

На сервере, в свою очередь, необходимо несколько раз запустить некоторый алгоритм генерации случайных чисел и обычные операции сложения и умножения (временные затраты на эти шаги незначительны). Кроме того, он запускает *n*

хэш-функций, а также значительные операции по генерации и проверке цифровых подписей в блоках и $n + 1$ раз просчитывает по расширенному Евклидову алгоритму.

Поэтому обработка операции на сервере требует следующих временны́х затрат:

$$T_S = nT_h + T_{SigServ} + (n + 1)T_{inv},$$

где T_{inv}, $T_{SigServ}$ – временны́е затраты на выполнение одного расширенного Евклидова алгоритма и на генерацию с проверкой цифровых подписей в блоках, состоящих из сложений и умножений случайных чисел в рамках криптографических алгоритмов [9].

Сетевую задержку при прохождении цикла транзакций между сервером и аутентифицирующими органами власти можно представить в виде выражения:

$$T_{Net} = (n^2 + 2n)T_{com},$$

где T_{com} – сетевая задержка при передаче одного сообщения между сервером и одним из аутентифицирующих органов власти; n – число аутентифицирующих органов власти; необходимо передать синхронизирующую транзакцию ($2n$), а также обновлять информацию при аутентификации каждым ведомством запроса (n^2).

Таким образом, можно представить результирующее время выполнения процедуры в следующем виде:

$$T_{Proc} = 2\sum_{i=1}^{n} T_{Ai} + n^2 T_S + T_{Net}.$$

Для оценки значения временных затрат на выполнение предложенной схемы был использован персональный компьютер (RedmiBook с процессором AMD Ryzen 5 5600H с графикой Radeon @ 3,30 ГГц с 16,0 ГБ оперативной памяти и ОС Windows 10 Home). В рамках имитации была предложена схема взаимодействия с различным числом полномочных органов власти. Для этого была развернута система смарт-контракта с использованием языка Solidity и Ropsten Ethereum [10] для тестирования сети с рядом предустановленных параметров. Компилятором языка Solidity является Remix IDE и его версия 0.7.4.

В рамках схемы множественной аутентификации пользователей были обозначены основные этапы: установка (MA-FS.Setup), генерация ключа (MA-FS.KeyGen), подпись (MA-FS.Sign) и проверка (MA-FS.Verify).

На этапе установки сервер сначала выбирает параметр безопасности λ и запускает алгоритм настройки подписи ECDSA для генерации публичных параметров, затем случайным образом выбирает главный закрытый ключ (Msk) и вычисляет главный открытый ключ (Mvk).

На этапе генерации ключа производится формирование и обмен парами открытого и закрытого ключей схемы между сервером и каждым аутентифицирующим ведомством. Процессы генерации ключей функционируют в соответствии с алгоритмом ECDSA (*аббр. от англ.* Elliptic Curve Digital Signature Algorithm – алгоритм построения цифровой подписи с использованием эллиптических кривых). Для каждого аутентифицирующего ведомства формируется его sk_f^i.

Этап подписи – для подписания сообщения каждое аутентифицирующее ведомство принимает на вход приватный ключ sk_f^i и формирует дополнительные параметры для генерации подписи сообщения sig_i. Сервер получает sig_i от всех аутентифицирующих ведомств и формирует базу для их хранения.

На этапе проверки для каждого аутентифицирующего ведомства производится проверка подписи, при этом верификатор данных может проверить подпись sig_i, используя алгоритм проверки подписи ECDSA, с учетом параметров каждого отдельного участника.

Операции в каждой модели выполнялись по 1000 раз, и в последующем были вычислены средние значение конечных результатов времени исполнения смарт контракта. Результаты эксперимента приведены на рисунке 10. Можно видеть, что время выполнения предложенной схемы блокчейн увеличивается по мере роста числа полномочных органов власти, участвующих в аутентификации запросов.

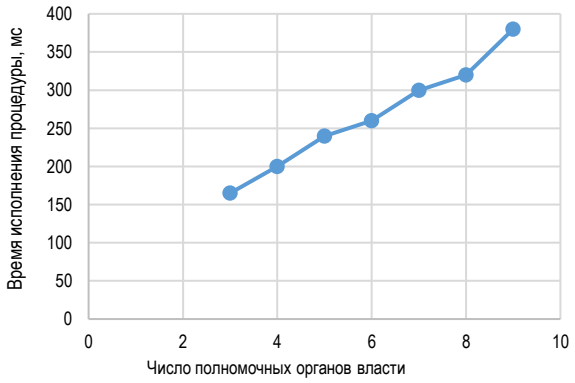

Рис. 10. Результаты моделирования схемы использования блокчейн при наличии более одного аутентифицирующего ведомства

Fig. 10. The Results of Modeling the Blockchain Scheme with More than One Authenticating Agency

Поскольку все больше и больше моделей аутентификации данных с использованием блокчейн находят свое распространение, представляется целесообразным применение схемы функциональных подписей запросов с участием нескольких сторон (полномочных органов) при большом их количестве. Благодаря особенностям организации блокчейн,

схема защищена от подделок и злоупотребления соответствующими инспекторами. Кроме того, имитационное моделирование показало производительность исследуемой схемы с точки зрения задержки по включению и авторизации запроса в цепочку для возможных проверок: около 164,81 мс для трех, 259,30 мс для шести и 388,68 мс для девяти полномочных органов власти.

Вывод

Интеграция технологий блокчейн в систему цифровых сервисов в рамках портала госуслуг РФ имеют очевидную перспективу. В первую очередь, это связано с переориентацией системы госуправления на «цифровое государство».

Использование блокчейна может перевести саму идею электронного правительства на новый уровень. Речь должна идти уже не просто об удобном сервисе предоставления гражданам и бизнесу, а о принципиальном переформатировании самой деятельности государства в контексте безопасности, полном погружении ее в цифровую экосистему блокчейна.

В статье была проанализирована работа технологии блокчейн, построена аналитическая модель ее взаимодействия с порталом ГИС, которая в свою очередь характеризует взаимодействие между узлами сети: блокчейн-узлами и государственными серверами. На основе аналитической модели произведена разработка имитационной модели, позволяющей оценить размер временны́х задержек для обработки запросов при увеличении числа полномочных органов власти для подтверждения его для включения в цепочку блокчейн.

Так как моделирование работы системы проводилось на одном аппаратном сервере с выделением соответствующего числа виртуальных машин, то сетевая задержка составляет единицы микросекунд, и ее вклад в общее время реализации процедуры ничтожно мал, однако стоит учитывать, что в реальных системах с территориально распределенными аутентифицирующими органами власти этот параметр может быть значительно выше.

Кроме того, в статье предложено использование известного метода реализации схемы цифровой подписи ECDSA, широко применяемого в блокчейн с внесением дополнительного сервера для обеспечения многопользовательской аутентификации сообщений в рамках смарт-контракта различными ведомствами.

Представленные в статье основные подходы и решения в рамках блокчейн, на базе которых возможно внедрение этой технологии в ГИС, в частности – портал государственных услуг, указывают на технологическую возможность внедрения технологии блокчейн при минимальном влиянии на временные сетевые характеристики системы и с поддержкой многопользовательской аутентификации услуг различными ведомствами.

Здесь стоит отметить, что для полноценного внедрения необходимо еще решить ряд вопросов, связанных с оценкой объемов трафика и команд, необходимых для работы с услугами. Дополнительно следует оценить возможность применения территориально распределенного сервера аутентификации, с учетом иерархической структуры самого портала Госуслуг и СМЭВ, с сохранением быстродействия, безопасности формирования блокчейн-транзакций и их защиты.

Отдельно стоит рассмотреть возможность применения технологии сегментирования в блокчейн для ГИС. Разделение на сегменты позволяет увеличивать пропускную способность по мере расширения сети валидаторов, что неизбежно при текущем развитии госуслуг; однако взаимодействие между сегментами может потребовать дополнительных ресурсов на синхронизацию, т. е. времени, чтобы вновь добавленные узлы загрузили последнее состояние. Потенциал и недостатки этой субтехнологии для внедрения также еще предстоит оценить.

Список источников

1. Госуслуги. URL: https://www.gosuslugi.ru (дата обращения 20.12.2022)
2. Зараменских Е.П. Цифровая трансформация государственных услуг // XIII Международная научно-практическая конференция «Государство и бизнес. Современные тенденции и проблемы развития экономики» (Санкт-Петербург, Россия, 21–22 апреля 2021). Санкт-Петербург: Северо-Западный институт управления – филиал РАНХиГС, 2021. С. 23–32.
3. Government as a Platform // Fujitsu Services. 2015. URL: https://www.fujitsu.com/uk/Images/government-as-a-platform.pdf (дата обращения 20.12.2022)
4. Система межведомственного электронного взаимодействия (СМЭВ) // TAdviser. 2022. URL: tadviser.ru/index.php/Продукт:Система_межведомственного_электронного_взаимодействия_(СМЭВ) (дата обращения 20.12.2022)
5. 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 (ICUMT, Brno, Czech Republic, 05–07 *October* 2020). IEEE, 2020. PP. 242–247. DOI:10.1109/ ICUMT51630.2020.9222437
6. 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 // T-Comm: Телекоммуникации и транспорт. 2020. Том 14. № 4. С. 39–45. DOI:10.36724/2072-8735-2020-14-4-39-45

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 // Proceedings of the Systems of Signals Generating and Processing in the Field of on Board Communications (Moscow, Russia, 19–20 March 2020). IEEE, 2020. P. 9078572. DOI:10.1109/ IEEECONF48371.2020.9078572
8. Memon R.A., Li J.P, Ahmed J. Simulation Model for Blockchain Systems Using Queuing Theory // Electronics. 2019. Vol. 8. Iss. 2. P. 234. DOI:10.3390/electronics8020234
9. 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 Communications (St. Petersburg, Russia, 21–23 June 2017). Lecture Notes in Computer Science. Vol. 10372. PP. 233–246. Cham: Springer, 2017. DOI:10.1007/978-3-319-61382-6_19
10. Ropsten Testnet Explorer // Etherscan. URL: https://ropsten.etherscan.io (дата обращения 20.06.2022)

References

1. *Gosuslugi*. (in Russ.) URL: https://www.gosuslugi.ru [Accessed 20th December 2022]
2. Zaramenskikh E. Digital Transformation of Government Services. Государство и бизнес. *Proceedings of the XIII International Scientific-Practical Conference on Current Trends and Problems of Economic Development, 21–22 April 2021, Saint Petersburg, Russia.* Saint-Petersburg: North-West Institute of Management of RANEPA Publ.; 2021. PP. 23–32. (in Russ.)
3. *Fujitsu Services.* Government as a Platform. 2015. URL: https://www.fujitsu.com/uk/Images/government-as-a-platform.pdf [Accessed 20th December 2022]
4. *TAdviser*. Interagency Electronic Interaction System. 2022. (in Russ.) URL: tadviser.ru/index.php/Продукт: Система_межведомственного_электронного_взаимодействия_(СМЭВ) [Accessed 20th December 2022]
5. 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, ICUMT, 05–07 October 2020, Brno, Czech Republic*. IEEE; 2020. p.242–247. DOI:10.1109/ICUMT51630. 2020.9222437
6. 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;14(4):39–45. (in Russ.) DOI:10.36724/2072-8735-2020-14-4-39-45
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. *Proceedings of the Systems of Signals Generating and Processing in the Field of on Board Communications, 19–20 March 2020, Moscow, Russia*. IEEE; 2020. p.9078572. DOI:10.1109/IEEECONF48371. 2020.9078572
8. Memon R.A., Li J.P, Ahmed J. Simulation Model for Blockchain Systems Using Queuing Theory. *Electronics*. 2019;8(2):234. DOI:10.3390/electronics8020234
9. 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 Communications, 21–23 June 2017, St. Petersburg, Russia. Lecture Notes in Computer Science, vol.10372*. p.233–246. Cham: Springer; 2017. DOI:10.1007/978-3-319-61382-6_19
10. *Etherscan*. Ropsten Testnet Explorer. URL: https://ropsten.etherscan.io [Accessed 20th June 2022]

Статья поступила в редакцию 09.09.2022; одобрена после рецензирования 05.12.2022; принята к публикации 16.12.2022.
The article was submitted 09.09.2022; approved after reviewing 05.12.2022; accepted for publication 16.12.2022.

Информация об авторе:

ЕЛАГИН Василий Сергеевич
кандидат технических наук, доцент кафедры Инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
https://orcid.org/0000-0003-4077-6869