

УДК 004.042

DOI: 10.18413/2518-1092-2020-5-3-0-5

Гончаренко Ю.Ю.
Арзамасцев Д.А.**ПРОГРАММНЫЙ МОДУЛЬ ДЛЯ КОНТРОЛЯ И ВЕДЕНИЯ
ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН**

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

*e-mail: iuliy1985@mail.ru, dan_arz@mail.ru***Аннотация**

Электронный документооборот является наиболее быстрым и качественным способом передачи информации на производстве в современных условиях работы. Технология же блокчейн, в свою очередь, может представлять собой надежный механизм для организации информационной безопасности в условиях ведения электронного документооборота, предоставляя значительные преимущества, такие как обеспечение проверки авторства и целостности передаваемых сведений. В статье приведен обзор особенностей ведения электронного документооборота и характеристика технологии блокчейн. Подняты проблемы обеспечения информационной безопасности и законности ведения электронного документооборота и обоснована возможность использования технологии блокчейн для реализации данных целей. Приведены принцип работы технологии блокчейн, описаны проблемы, возможные к возникновению при ее использовании и возможные их решения. Описан алгоритм работы разработанного программного модуля для контроля и ведения электронного документооборота на основе технологии блокчейн с приведением требований для корректной его работы. Разработанное решение имеет преимущества по сравнению с обычной реализацией ведения электронного документооборота, поскольку помимо автоматизации данного процесса является также и механизмом обеспечения информационной безопасности.

Ключевые слова: электронный документооборот; технология блокчейн; информационная безопасность; программная реализация.

UDC 004.042

Goncharenko J.Y.
Arzamastsev D.A.**SOFTWARE MODULE FOR MONITORING AND MAINTAINING
ELECTRONIC DOCUMENT MANAGEMENT BASED
ON BLOCKCHAIN TECHNOLOGY**

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

*e-mail: iuliy1985@mail.ru, dan_arz@mail.ru***Abstract**

Electronic document management is the fastest and most high-quality way of transmitting information in production in modern working conditions. Blockchain technology, in turn, can be a reliable mechanism for organizing information security in electronic document management, providing significant advantages, such as providing verification of authorship and the integrity of the information transmitted. The article provides an overview of the features of electronic document management and a characteristic of blockchain technology. The problems of ensuring information security and the legality of electronic document management have been raised and the possibility of using blockchain technology to achieve these goals has been substantiated. The principle of operation of the blockchain technology is described, the problems that may arise during its use and their possible solutions are described. The algorithm of the developed software module for monitoring and maintaining electronic document management based on blockchain technology with requirements for its correct operation is described. The developed solution has advantages compared to the usual implementation of electronic document management, because in addition to automating this process, it is also a mechanism for ensuring information security.

Keywords: electronic document management; blockchain technology; Information Security; software implementation.

ВВЕДЕНИЕ

Электронный документооборот – это явление, получившее в последнее время широкое распространение благодаря значительному упрощению процессов создания, передачи и редактирования информации, как для рядового пользователя персонального компьютера, так и для крупных компаний, предоставляющих свои услуги во всевозможных сферах деятельности, актуальных для современного общества.

Однако, совместно с ростом количества способов возможной передачи информации и развитием методов ее передачи возникают также и существенные риски, касающиеся обеспечения информационной безопасности. До сих пор, например, одним из наиболее часто используемых злоумышленниками вектором атаки является компьютерный взлом, в основном из-за легкости своего осуществления и повышенного интереса к хранимой информации.

Существует множество технологий и способов обеспечения информационной безопасности, однако, в данный момент, интересом в области оказания подобных услуг пользуются практически реализованные технологии блокчейн, начавшие пользоваться спросом несколько лет назад и уже доказавшие свою эффективность путем повышения качества жизни множества людей за счет разнообразных применений в большинстве аспектов современной жизни. Например, в настоящее время технология блокчейн активно используется в следующих областях: обеспечение работы криптовалют, смарт-контракты, обеспечение цепочки поставок, регистрация доменных имен; проведение онлайн-голосований, страхование, удостоверение личности [Singh N., 2019]. В июне 2017 года компании Accenture и Microsoft представили систему, реализованную при помощи технологии блокчейн, позволяющую идентифицировать человека и выдать цифровое удостоверение [Accenture, 2017], а уже в мае 2019 года компания Amazon реализовала и открыла собственный сервис, позволяющий клиентам при заключении договора получить собственный сервер и значительно упростить ведение блокчейна. На данный момент, среди их клиентов находятся Philips, Sony Music, Verizon и иные компании [Amazon Web Services, 2018].

Учитывая подобный стремительный рост использования данной технологии и широту спектра ее возможного применения, она способна не только обеспечить повышение информационной безопасности данных, но также и рост уровня оказываемых услуг, предоставляя пользователям большое количество возможностей своего использования.

ОСОБЕННОСТИ ВЕДЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

Электронный документооборот – это обмен электронными документами по доступным каналам связи, как внутри предприятия, так и вне его [DOCFLOW, 2017].

Электронный документ – это файл или любая иная информация, представленная в цифровом виде, хранящаяся/передающаяся в пределах какой-либо информационной системы.

Понятия электронного документооборота или электронного документа не приводятся в нормативно-правовых документах, однако активно используются, что показывает распространенность и удобство в освоении электронного документооборота и может послужить доказательством его активного использования в практических вопросах.

К нормативно-правовым документам, регулирующим вопросы электронного документооборота можно отнести Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» и Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», поскольку в них описываются основные понятия данного вопроса, такие как «информация», способы ее передачи и регулируются требования к электронной цифровой подписи, позволяющие организовывать электронный документооборот на предприятии [Информационная система 1С:ИТС, 2020].

Документом, обеспечивающим законность ведения электронного документооборота при условии подписания сообщений электронной цифровой подписью, является Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». А именно, в статье 7 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» «Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами» приведено нижеследующее.

Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании Федерального закона [КонсультантПлюс, 2020].

Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права [КонсультантПлюс, 2020].

Для обеспечения реализации этих целей также может использоваться и технология блокчейн, поскольку способна обеспечить проверку авторства и целостности любых данных или документа, передающихся в сети.

Блокчейн – это цепочка блоков информации заранее определенного содержания, созданных по заранее определенным правилам или любых других записей, сообщений или сведений, необходимых для сохранения, передачи и просмотра [Блокчейн, 2020].

Один блок блокчейна является специальной структурой, созданной для хранения сведений об одном, или любом другом, определенном заранее, количестве событий, сообщений или любом другом представлении определенной информации. Содержимое любого блока блокчейна всегда может быть просмотрено, а информация проверена на подлинность путем сравнения с информацией, представленной в соответствующем блоке блокчейна.

Каждый блок блокчейна, кроме родительского, необходимого только лишь для поддержания работоспособности технологии, содержит в себе информацию заранее определенного содержания, в зависимости от необходимости применения технологии, области ее применения и иных факторов. Однако, в независимости от перечисленных факторов, в блоке всегда присутствует следующая информация:

- номер блока;
- хеш предыдущего блока;
- информация для сохранения;
- хеш данного блока [Щербань Е, 2017].

У данной технологии существует лишь одна проблема, возникающая в ходе ее использования, а именно – проблема возникновения параллельных ветвей, что означает создание последовательности блоков блокчейна, состоящей из одного или более блока, продолжающейся путем добавления в блокчейн блоков к блоку главной ветви. Такие ветви, как правило, образуются при желании злоумышленников изменить представление остальных пользователей сети об информации, находящейся в одном из блоков блокчейна для достижения личных целей [Hooda P., 2020].

Данная проблема, однако, легко решается на практике путем использования механизмов защиты таких как PoW (Proof of Work) (доказательство работой), PoB (Proof of Burn) (доказательство уничтожением), PoS (Proof of Stake) (доказательство долей), PoC (Proof of Capacity) (доказательство объемом), PoET (Proof of Elapsed Time) (доказательство затраченным временем) или простым игнорированием возможной параллельной ветви иными пользователями сети [Sharma T., 2018].

Таким образом, технология блокчейн является крайне гибкой технологией, доступной к реализации для решения огромного спектра задач и способна значительно упростить некоторые процессы и аспекты жизни человека, а некоторые – существенно улучшить путем решения

множества современных проблем, в том числе и за счет обеспечения информационной безопасности.

ОПИСАНИЕ РАБОТЫ ПРОГРАММНОГО МОДУЛЯ

Разработанный программный модуль для контроля и ведения электронного документооборота на основе технологии блокчейн позволяет обеспечить реализацию электронного документооборота в локальной сети, поддерживая передачу и обеспечение целостности сообщений и передаваемых файлов, также обеспечивая проверку авторства.

Для корректной работы программного модуля на компьютере конечного пользователя должен быть установлен язык программирования Python версии 3.7.1 или более и следующие модули данного языка:

- socket;
- threading;
- os;
- hashlib;
- ntplib;
- time;
- datetime;
- easygui.

Модуль socket позволяет в ходе работы программы создавать сокет (начальные или конечные точки коммуникации) из пары значений IP-адреса и сетевого порта компьютера, производить подключения и передавать данные между ними.

Модуль threading позволяет в ходе работы программы создавать или удалять отдельные потоки выполнения программного кода, обеспечивая таким образом многопоточность программы, значительно сокращая время ее выполнения.

Модуль os позволяет в ходе работы программы обеспечить возможность выполнения базовых функций операционной системы путем вызова соответствующих команд в командной строке.

Модуль hashlib позволяет в ходе работы программы обеспечить выполнение криптографических хеш-функций, указывая входные данные и получая выходные данные соответствующих алгоритмов хеширования.

Модуль ntplib позволяет в ходе работы программы получить точное время, включая доли секунд, для различных часовых поясов путем формирования и отправки запроса к проекту Network Time Protocol и получения ответа в виде метки времени.

Модуль time позволяет в ходе работы программы получить сведения о текущих времени и дате, используя системные часы, а также приостановить работу программы на определенный промежуток времени путем вызова функции sleep, для чего, как правило, и используется, обеспечивая, например, определенный период ожидания в ходе выполнения программы для сохранения ресурсов.

Модуль datetime позволяет в ходе работы программы, как и модуль time, получить сведения о текущих времени и дате, используя системные часы, однако предоставляет гораздо более расширенный функционал для выполнения различного спектра задач, а также позволяет изменять формат меток времени, предоставляя их более понятным для восприятия путем.

Модуль easygui позволяет в ходе работы программы обеспечить создание, появление и сбор данных через элементы графического интерфейса, что способствует более комфортному использованию программы конечным пользователем.

Модули socket, threading, os, hashlib, time и datetime поставляются совместно с языком программирования Python, однако модули ntplib и easygui должны быть установлены перед началом работы программы путем выполнения команды «python -m pip install ntplib» в командной строке операционной системы.

Помимо этого, рекомендуется полученный исполняемый файл поместить в любую директорию, изначально не содержащую в себе папку «files» и файлы chain.txt и tempchain.txt, иначе файлы будут перезаписаны, а в папка «files» будет в дальнейшем использоваться как служебная папка программы.

При разработке программного модуля были учтены вопросы обеспечения информационной безопасности при работе с технологией блокчейн. Из-за этого, при любом обнаружении несоответствия уже имеющихся данных в блокчейне пользователя в сравнении его с блокчейном другого пользователя это будет свидетельствовать о возникновении параллельной ветви блокчейна, что может подразумевать появление злоумышленника в локальной сети. Участник сети с различающимся блокчейном не сможет передать его иному пользователю ни при каких обстоятельствах, а пользователю, инициировавшему проверку или обновление блокчейна, будь это любой из этих пользователей в ближайшем диалоговом окне будет рекомендовано обратиться к вышестоящему лицу.

В начале своего выполнения разработанный программный модуль подключает библиотеки, необходимые для его работы, и представляет пользователю поочередно два диалоговых окна, предназначенных для ввода локального IP-адреса компьютера пользователя и для ввода IP-адресов иных компьютеров в локальной сети, проверяет наличие папки «files» и файла chain.txt и, в случае их отсутствия создает их. Далее выполняется основной цикл программы.

Выполнение основного цикла программы сопровождается появлением главного меню программного модуля. При первом выполнении цикла главное меню, помимо основного текста, будет содержать следующий: «Рекомендуемая операция: обновить блокчейн», тогда как при последующих выполнениях (после первого выбора операции пользователем) главное меню будет содержать только основной текст: «Пожалуйста, выберите необходимую операцию:» (рис. 1).

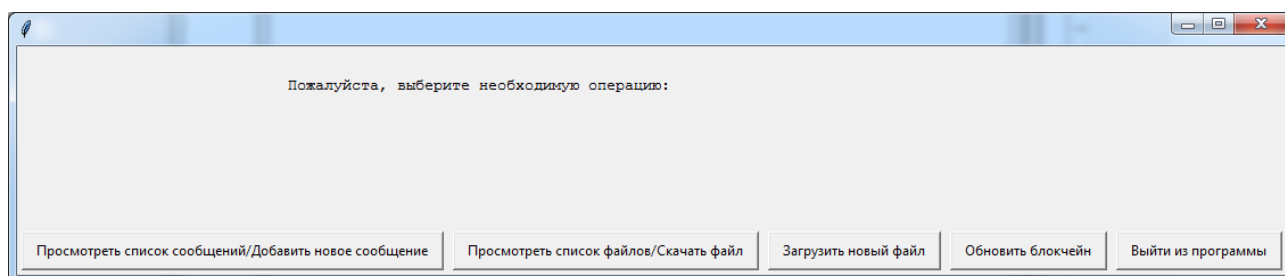


Рис. 1. Главное меню программного модуля
Fig. 1. The main menu of the software module

При выборе пользователем опции «Просмотреть список сообщений/Добавить новое сообщение» из главного меню, возникнет окно сообщений, содержащее текст «К сожалению, никто еще не добавлял сообщения» или список сообщений с указанием локального IP-адреса компьютера отправителя каждого сообщения. Окно сообщений всегда будет содержать опции «Добавить новое сообщение» и «Вернуться в главное меню» (рис. 2).

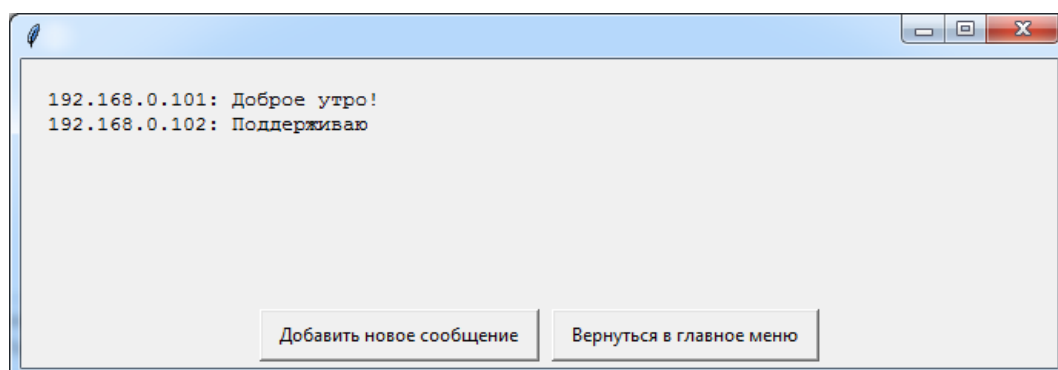
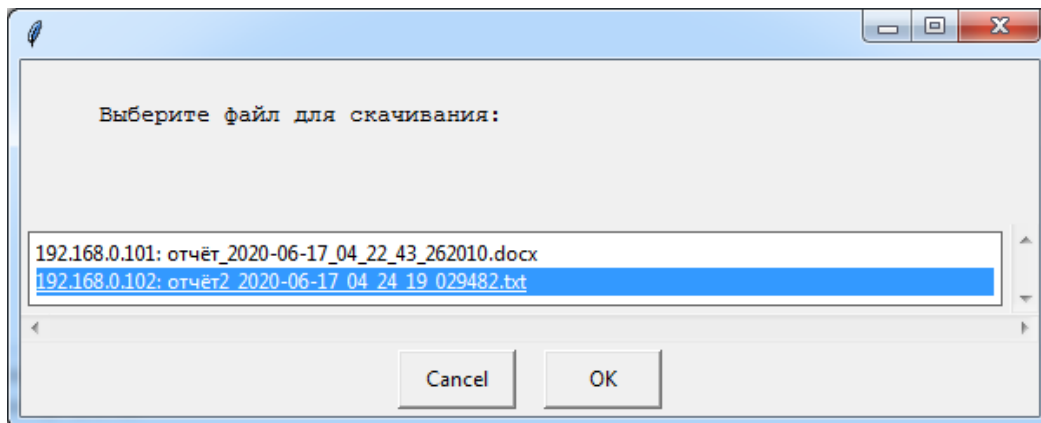


Рис. 2. Окно сообщений
Fig. 2. Message window

При выборе пользователем опции «Добавить новое сообщение» возникнет диалоговое окно с полем для ввода сообщения. После ввода сообщения пользователем блокчейн будет обновлен и разослан всем участникам сети, чьи локальные IP-адреса были указаны ранее. После добавления сообщения в блокчейн или при выборе пользователем на любом этапе опции отмены произойдет возврат в главное меню.

При выборе пользователем опции «Просмотреть список файлов/Скачать файл» из главного меню, возникнет диалоговое окно, содержащее список файлов, когда-либо добавленных в блокчейн всеми пользователями сети с указанием локального IP-адреса компьютера, хранящего файл (рис. 3).



*Рис. 3. Окно со списком файлов
Fig. 3. Window with a list of files*

При выборе пользователем файла для скачивания возникнет диалоговое окно, предлагающее выбрать имя и путь для сохранения файла, далее произойдет подключение к компьютеру, хранящему данный файл и его загрузка. В случае, если файл, выбранный пользователем изначально был загружен им же возникнет диалоговое окно, предлагающее продолжить или отменить загрузку файла. В случае выбора пользователем варианта продолжить загрузку файл будет скопирован из служебной папки «files».

Результаты загрузки файла будут показаны пользователю в дальнейшем диалоговом окне. После загрузки файла или при выборе пользователем на любом этапе опции отмены произойдет возврат в главное меню.

При выборе пользователем опции «Загрузить новый файл» из главного меню, возникнет диалоговое окно, предлагающее выбрать пользователю файл для добавления его в блокчейн. После выбора файла произойдет его копирование в служебную папку «files», с дальнейшим добавлением информации об этом файле в блокчейн и рассылке блокчейна всем пользователям сети.

При выборе пользователем опции «Обновить блокчейн» из главного меню, произойдет процесс обновления блокчейна пользователя, который подразумевает нахождение иного пользователя локальной сети с длиннейшим файлом блокчейна и копирование информации из него. Однако, если уже имеющиеся данные в блокчейне пользователя, запросившего обновление, различны обновления блокчейна не произойдет. После выполнения данного процесса возникнет диалоговое окно, уведомляющее пользователя об обновлении или причинах невозможности обновления его блокчейна (рис. 4).

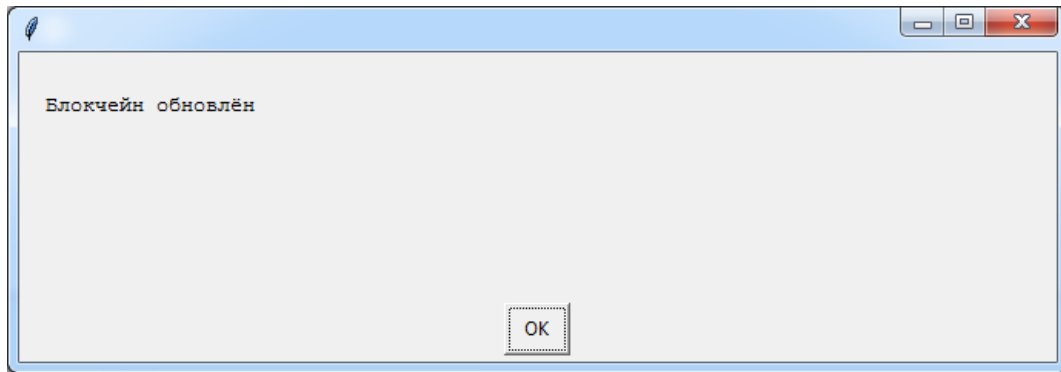


Рис. 4. Успешное обновление блокчейна

Fig. 4. Successful blockchain update

При выборе пользователем опции «Выйти из программы» из главного меню, произойдет ожидание завершения всех параллельных потоков, созданных в процессе работы программы и завершение работы основного цикла программы, что приведет к выходу из нее.

В ходе работы программы при рассылке блокчейна после добавления в него каких-либо данных всегда возникнет окно, содержащее результаты рассылки блокчейна для всех пользователей сети с указанием их IP-адресов и соответствующих результатов (рис. 5).

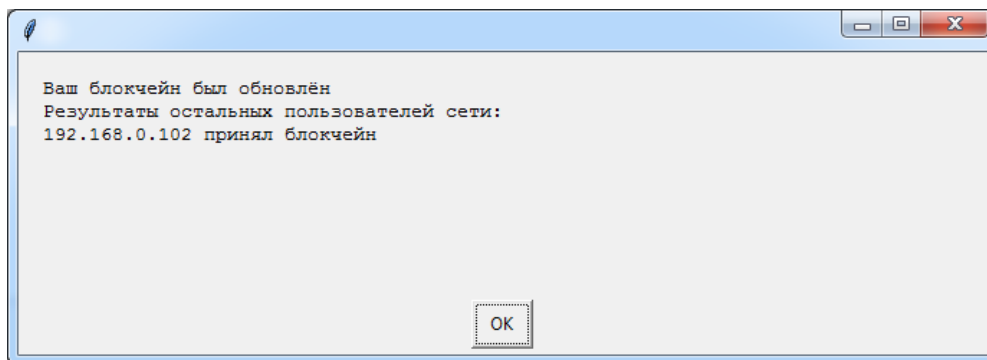


Рис. 5. Окно с результатами рассылки блокчейна

Fig. 5. Window with the results of blockchain distribution

Помимо этого, в ходе работы программы при успешном обновлении блокчейна, если инициатором обновления являлся другой пользователь сети, вне зависимости от текущего этапа выполнения программы всегда возникнет окно, уведомляющее об обновлении блокчейна.

Пример файла блокчейна, дополнявшегося записями в ходе работы программного модуля представлен на рисунке 6.

```

chain.txt — Блокнот
Файл  Правка  Формат  Вид  Справка
Block:Genesis
Content_type:
Author:
Content:
Content_hash:
Prev_hash:
Hash:beb1e87ee30222c7790a8a8d14c3a702985f3958d80ef8712db6219e491d2d54

Block:1
Content_type:file
Author:192.168.0.101
Content:отчет_2020-06-17_04_22_43_262010.docx
Content_hash:2f2b134312808a9051927575a59886711cbf7fb6e3b8ee1e49c53b2175bbaa3c
Prev_hash:beb1e87ee30222c7790a8a8d14c3a702985f3958d80ef8712db6219e491d2d54
Hash:0ed02c4573318c261115a936ed882c9451396ef0694166b3c2412a228075a20f

Block:2
Content_type:file
Author:192.168.0.102
Content:отчет2_2020-06-17_04_24_19_029482.txt
Content_hash:370897b6c4954d7ca14dfe57554dbd85c7e03b055996fcfb86431e3a195801f
Prev_hash:0ed02c4573318c261115a936ed882c9451396ef0694166b3c2412a228075a20f
Hash:c172b16022b54b49ad74f32b86defcb532f88662df4189994ea02cecd1e5f49e

Block:3
Content_type:message
Author:192.168.0.101
Content:доброе&утро!2020-06-17_04_25_52_242557
Content_hash:154a0236206c5b264bec3a6fc2197c5570086d1de161aabcd50d5895776f27e8
Prev_hash:c172b16022b54b49ad74f32b86defcb532f88662df4189994ea02cecd1e5f49e
Hash:2fcc14ddb841e689dfc793b14f7355e8dce57e53cbb432bf09e1e5c0110a2870

Block:4
Content_type:message
Author:192.168.0.102
Content:поддерживаю2020-06-17_04_26_31_957408
Content_hash:1766e8146847a81376479f1543da2347fcbd8284dfea687eb0edb698c94d876e
Prev_hash:2fcc14ddb841e689dfc793b14f7355e8dce57e53cbb432bf09e1e5c0110a2870
Hash:16c51de8e90ccb9f8feb1787665c0ec704ea43f9dea40a3e2552b65249095d61
    
```

Рис. 6. Файл блокчейна

Fig. 6. Blockchain file

ЗАКЛЮЧЕНИЕ

Таким образом, разработанный программный модуль для контроля и ведения электронного документооборота на основе технологии блокчейн обладает возможностями значительно ускорить процесс передачи информации в сети, убедиться в ее получении иными пользователями сети и способен предоставить должный уровень защиты информации при ведении электронного документооборота за счет использования преимуществ технологии блокчейн.

Список литературы

1. Блокчейн, 2020. URL: <https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD> (дата обращения: 02.05.2020).
2. Информационная система 1С: ИТС, 2020. Правовые основы обмена электронными документами. URL: <https://its.1c.ru/db/eldocs#content:3:hdoc> (дата обращения: 01.05.2020).
3. КонсультантПлюс, 2020. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи». URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=354532> (дата обращения: 01.05.2020).
4. Щербань Е, 2017. Что такое блокчейн, и как это работает. URL: <https://revolverlab.com/how-its-works-blockchain-6d0355c43bfc> (дата обращения: 03.06.2020).

5. DOCFLOW, 2017. Электронный документооборот: что такое электронный документооборот, основные понятия, виды, преимущества, задачи, критерии выбора, классификация систем, требования. URL: <http://www.docflow.ru/edu/glossary/detail.php?ID=27946> (дата обращения: 01.06.2020).
6. Accenture, 2017. Accenture, Microsoft Create Blockchain Solution to Support ID2020. URL: <https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm> (дата обращения: 04.05.2020).
7. Amazon Web Services, 2018. Amazon Managed Blockchain. URL: <https://aws.amazon.com/ru/managed-blockchain/> (дата обращения: 04.05.2020).
8. Hooda P., 2020. Blockchain Forks. URL: <https://www.geeksforgeeks.org/blockchain-forks/> (дата обращения: 03.05.2020).
9. Singh N., 2019. Blockchain Usage: List of 20+ Blockchain Technology Use Cases. URL: <https://101blockchains.com/blockchain-usage/> (дата обращения: 04.05.2020).
10. Sharma T., 2018. What are the alternative strategies for Proof-Of-Work? URL: <https://www.blockchain-council.org/blockchain/what-are-the-alternative-strategies-for-proof-of-work/> (дата обращения: 04.05.2020).

References

1. Blockchain, 2020. URL: <https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD> (access date: 02/06/2020).
2. Information system 1C: ITS, 2020. Legal basis for the exchange of electronic documents. URL: <https://its.1c.ru/db/eldocs#content:3:hdoc> (access date: 01/06/2020).
3. ConsultantPlus, 2020. Federal Law of 06.04.2011 N 63-ФЗ «On electronic signature». URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=354532> (access date: 01/06/2020).
4. Shcherban E, 2017. What is blockchain and how does it work. URL: <https://revolverlab.com/how-its-works-blockchain-6d0355c43bfc> (access date: 03/06/2020).
5. DOCFLOW, 2017. Electronic document management: what is electronic document management, basic concepts, types, advantages, tasks, selection criteria, classification of systems, requirements. URL: <http://www.docflow.ru/edu/glossary/detail.php?ID=27946> (access date: 01/06/2020).
6. Accenture, 2017. Accenture, Microsoft Create Blockchain Solution to Support ID2020. URL: <https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm> (access date: 04/06/2020).
7. Amazon Web Services, 2018. Amazon Managed Blockchain. URL: <https://aws.amazon.com/ru/managed-blockchain/> (access date: 04/06/2020).
8. Hooda P., 2020. Blockchain Forks. URL: <https://www.geeksforgeeks.org/blockchain-forks/> (access date: 03/06/2020).
9. Singh N., 2019. Blockchain Usage: List of 20+ Blockchain Technology Use Cases. URL: <https://101blockchains.com/blockchain-usage/> (access date: 04/06/2020).
10. Sharma T., 2018. What are the alternative strategies for Proof-Of-Work? URL: <https://www.blockchain-council.org/blockchain/what-are-the-alternative-strategies-for-proof-of-work/> (access date: 04/06/2020).

Гончаренко Юлия Юрьевна, доктор технических наук, доцент, профессор кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Арзамасцев Даниил Аркадиевич, студент кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Goncharenko Julia Yurievna, Doctor of Technical Sciences, Associate Professor, Professor of the Department Information security, Institute of Radioelectronics and Information Security

Arzamastsev Daniil Arkadievich, student of the Department Information security, Institute of Radioelectronics and Information Security