УДК 004.043 Вестник УрФО № 1(47) / 2023, с. 98–101

Гончаренко Ю.Ю.

DOI: 10.14529/secur230109

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ПРОВЕРКИ ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ И ФАЙЛОВ

В данной статье предложено решение на основе распределенной децентрализованной технологии блокчейн для проверки подлинности электронной документации, проанализирована целесообразность использования и преимущества его внедрения.

На сегодняшний день проблема обеспечения подлинности электронных документов, особенно в их долговременной перспективе, является актуальной задачей, обеспечивающей безопасность обмена электронными данными за счет установления достоверности происхождения документа и целостности передаваемой информации.

В целях создания надежного верификационного центра для электронных документов и файлов было разработано веб-приложение, основанное на технологии блокчейн.

Ключевые слова: *блокчейн, электронный документ, верификация, веб-приложение.*

Goncharenko Y.Y.

USING BLOCKCHAIN TECHNOLOGY TO VERIFY THE AUTHENTICITY OF ELECTRONIC DOCUMENTS AND FILES

In this article, a solution based on distributed decentralized blockchain technology for verifying the authenticity of electronic documentation is proposed, the expediency of using it and the advantages of its implementation are analyzed.

To date, the problem of ensuring the authenticity of electronic documents, especially in their long-term perspective, is an urgent task that ensures the security of electronic data exchange by establishing the authenticity of the origin of the document and the integrity of the transmitted information.

In order to create a reliable verification center for electronic documents and files, a web application based on blockchain technology was developed.

Keywords: *blockchain, electronic document, verification, web application.*

Введение

В настоящее время во всём мире стремительно растет объем документооборота, что значительно расширяет спектр возможностей для злоумышленников по воздействию на какого-либо пользователя, например, таких, как кража данных, подделка документов и авторства и прочее. Это огромная проблема для широкой аудитории и еще большая проблема для предприятия с большим объемом циркулирующих данных [1].

Решением данной проблемы может быть внедрение технологии блокчейн в систему электронного документооборота, т. к. именно она способна защитить данные и сделать их аудит более прозрачным. Стремительность роста использования данной технологии и расширение спектра ее возможного применения позволяет не только обеспечить повышение информационной безопасности данных, но также и повысить уровень оказываемых услуг, предоставляя пользователям большое количество возможностей своего использования [2].

Таким образом, наличие специализированного средства подтверждения подлинности электронных документов и файлов, обусловленное необходимостью обеспечения целостности данных внутри них, является актуальной разработкой в сфере защиты информации. Такой подход к защите информации не позволит видоизменять передаваемые данные, поэтому информация в конечном виде будет полностью соответствовать сведениям, предоставленным и подтвержденным отправителем в изначальном виде [3].

Основная часть

Согласно п.11.1 ст.2 ФЗ «Об информации, информационных технологиях и о защите информации», электронный документ – это «документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах» [4].

При работе с электронными документами большое внимание уделяется гарантии их подлинности, для чего в системе электронного документооборота должны быть предусмотрены механизмы, гарантирующие защищённое хранение конфиденциальных документов, предотвращение несанкционированных изменений документов, копирование их содержимого [5]. Конечно, одним из распространенных способов подтвердить неизменность данных в документе и идентифицировать лицо, его подписавшее, является электронная подпись [6].

Но наличие проблем, связанных с ее использованием, не дают гарантий безопасности [7], поэтому в целях создания надежного верификационного центра для электронных документов и файлов было разработано веб-приложение, основанное на технологии блокчейн. Для написания более адаптивного и расширяемого приложения, было принято решение разделить его на логику взаимодействия пользователя с программным интерфейсом и на сам механизм блокчейна в серверной части приложения. Такая архитектура позволяет написать множество реализаций сценариев взаимодействия пользователя с API системой, например, мобильное приложение (рис. 1).

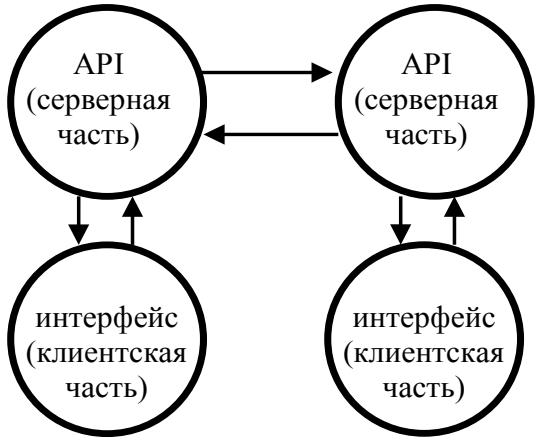

Рис. 1. Логика взаимодействия частей приложения

Основная идея заключается в возможности зарегистрированного пользователя загрузить в систему блокчейн хеш-сумму от документа (рис. 2).

После загрузки файла во временное хранилище веб-приложения происходит перевод файла в формат Base64. К полученной строке символов применяется функция хеширования SHA-256, а ее результат заносится в массив ожидающих транзакций. В свою очередь, пользователю выводится уведомление о добавлении хеш-суммы в блок цепочки блокчейн (рис. 3).

Для добавления нового блока, подтверждения транзакций и верификации единой версии реестра во всех его копиях нахождение консенсуса в системе осуществляется на

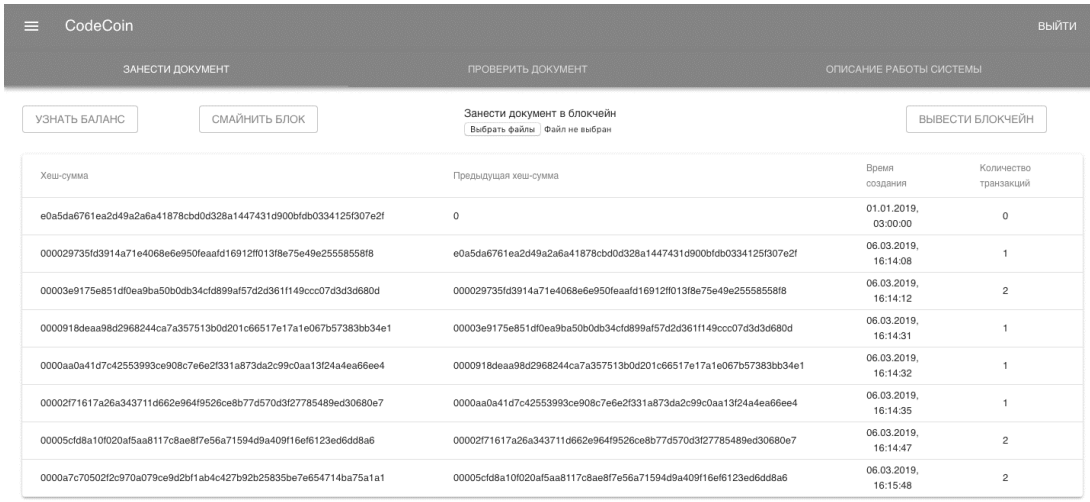

Рис. 2. Главная страница приложения

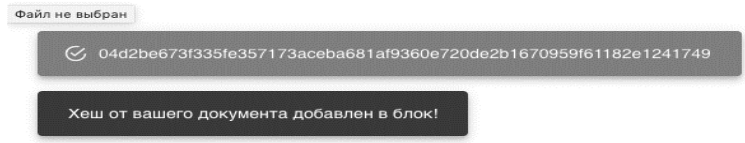

Рис. 3. Уведомление о добавлении в блок и хеш-сумма

основе алгоритма консенсуса Proof of Work (доказательство работы) [8]. Поэтому для закрытия блока и внесения его в цепочку необходимо подобрать такое число (nonce), при котором хеш-сумма от всего блока начиналась бы на «0000». Узлу, нашедшему требуемую хеш-сумму, начисляется 100 единиц (codecoin). При добавлении большого числа пользователей возможно увеличение количества нулей, что способствует росту вычислительной сложности закрытия блока.

После закрытия блока, пользователь всегда сможет удостоверится в том, что его документ был занесен в систему или, что он остался неизмененным. Для этого необходимо указать логин участника, создавшего документ, и ввести от него хеш-сумму. Если документ был зарегистрирован, то система покажет соответствующее уведомление, и есть возможность проверить целостность файла (рис. 4). Пользователь может повторно получить хеш-сумму от файла и проверить, зарегистрирован ли он.

В дальнейшем усовершенствовании системы для занесения документа будет требоваться небольшая сумма «codecoin», как оплата вычислительной мощности узлов, которые просчитывают хеш-функции. Уже на данный момент у зарегистрированных пользователей существуют кошельки с балансами, а также возможность передачи внутренней валюты другим пользователям (рис. 5).

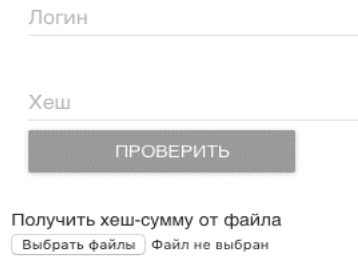

Рис. 4. Проверка файла

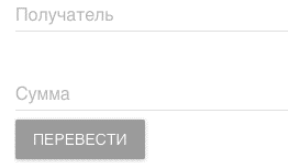

Рис. 5. Перевод codecoin

Выводы

Таким образом, разработанное веб-приложение, основанное на технологии блокчейн, представляет собой надежный верификационный центр для электронных документов и файлов, одним из преимуществ которого является отсутствие потребности хранить электронные копии документов на централизованном сервере, что в первую очередь исключает возможность получения доступа к ним злоумышленникам.

Данное приложение может быть использовано для упрощения взаимодействия между пользователями системы электронного документооборота, имеющими основание не доверять друг другу в вопросах подлинности совместно используемых данных.

Литература

1. Blockchain Usage: List Of 20+ Blockchain Technology Use Cases. – URL: https://101blockchains.com/blockchain-usage/ (дата обращение: 30.01.2023).

2. Гончаренко, Ю.Ю. Программный модуль для контроля и ведения электронного документооборота на основе технологии блокчейн / Ю.Ю. Гончаренко, Д.А. Арзамасцев // Научный результат. Информационные технологии. – Т.5, №3, 2020. – С. 32–40.

3. Гончаренко, Ю.Ю. Качественная оценка методик разработки автоматизированных средств / Ю.Ю. Гончаренко, Г.С. Погуляй, В.В. Пелись, М.Г. Щербаченко // Энергетические установки и технологии, 2022. – Т. 8. № 2. С. 79–86.

4. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями). – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращение: 30.01.2023).

5. Электронная подпись: что и зачем нужно настроить? – URL: https://docsvision.com/info-centr/articles/elektronnaya-podpis.html (дата обращение: 30.01.2023).

6. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 28.12.2022) «Об электронной подписи». – URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращение: 30.01.2023).

7. Проблемы использования электронной цифровой подписи. – URL: https://studbooks.net/2431093/informatika/problemy_ispolzovaniya_elektronnoy_tsifrovoy_podpisi (дата обращение: 30.01.2023).

8. Что такое алгоритм Proof-of-Work (PoW)? – URL: https://forklog.com/cryptorium/chto-takoe-proof-of-work-i-proof-of-stake (дата обращение: 30.01.2023).

References

1. Blockchain Usage: List Of 20+ Blockchain Technology Use Cases. – Available at: https://101blockchains.com/blockchain-usage/ (accessed 30 January 2023).

2. Goncharenko, YU.YU. Programmnyy modul' dlya kontrolya i vedeniya elektronnogo dokumentooborota na osnove tekhnologii blokcheyn / YU.YU. Goncharenko, D.A. Arzamastsev // Nauchnyy rezul'tat. Informatsionnyye tekhnologii. – T.5, №3, 2020. – S. 32–40.

3. Goncharenko, YU.YU. Kachestvennaya otsenka metodik razrabotki avtomatizirovannykh sredstv / YU.YU. Goncharenko, G.S. Pogulyay, V.V. Pelis', M.G. Shcherbachenko // Energeticheskiye ustanovki i tekhnologii, 2022. – T. 8. № 2. S. 79–86.

4. Federal'nyy zakon ot 27 iyulya 2006 g. N 149-FZ "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" (s izmeneniyami i dopolneniyami). – URL: https://www.consultant.ru/document/cons_doc_ LAW_61798/ (data obrashcheniye: 30.01.2023).

5. Elektronnaya podpis': chto i zachem nuzhno nastroit'? – URL: https://docsvision.com/info-centr/articles/elektronnaya-podpis.html (data obrashcheniye: 30.01.2023).

6. Federal'nyy zakon ot 06.04.2011 N 63-FZ (red. ot 28.12.2022) "Ob elektronnoy podpisi". – URL: https://www.consultant.ru/document/cons_doc_ LAW_112701/ (data obrashcheniye: 30.01.2023).

7. Problemy ispol'zovaniya elektronnoy tsifrovoy podpisi. – URL: https://studbooks.net/2431093/informatika/problemy_ispolzovaniya_elektronnoy_tsifrovoy_podpisi (data obrashcheniye: 30.01.2023).

8. CHto takoe algoritm Proof-of-Work (PoW)? Available at: https://forklog.com/cryptorium/chto-takoe-proof-of-work-i-proof-of-stake (accessed 30 January 2023).

ГОНЧАРЕНКО Юлия Юрьевна, доктор технических наук, доцент, профессор кафедры «Информационная безопасность», Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет». Россия, 299053, г. Севастополь, ул. Университетская, 33. E-mail: luliay1985@mail.ru

GONCHARENKO Yuliya Юрьевна, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "Sevastopol State University". 299053, Sevastopol, Universitetskaya Street, 33. E-mail: luliay1985@mail.ru