ДИАЛОГИ СО СПЕЦИАЛИСТАМИ

Научная статья
УДК 681.3; DOI: 10.61260/2304-0130-2025-1-46-50

ДЕЦЕНТРАЛИЗОВАННОЕ ХРАНЕНИЕ ИНФОРМАЦИИ

✉**Лабинский Александр Юрьевич.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***labinskyi.a@igps.ru***

Аннотация. Рассмотрены особенности и возможности децентрализованного хранения информации с помощью технологии блокчейн, алгоритм реализации хэш-функции, предназначенной для подсчета контрольной суммы, используемой для поддержания связи между блоками данных в распределенной базе данных, обеспечивающей децентрализованное хранение информации.

Рассмотрены проблемы блокчейн-технологии распределенных баз данных, типы архитектур распределенных баз данных на основе блокчейна и области применения блокчейн-технологии.

Подробно рассмотрен алгоритм циклического избыточного кода, используемый для подсчета контрольной суммы на основе входных данных, и реализация циклического избыточного кода в виде хэш-функции путем разработки алгоритма и программы для электронно-вычислительных машин.

Представлены блок-схема алгоритма подсчета контрольной суммы CRC-32 и консольная программа CRC32, реализующая данный алгоритм. Рассмотрен пример подсчета контрольной суммы для двух строк текста, в которых перестановка местами нескольких слов привела к изменению контрольной суммы.

Ключевые слова: децентрализованное хранение информации, распределенная база данных, блокчейн-технология, циклический избыточный код, контрольная сумма, хэш-сумма, хэш-функция, алгоритм, программа для ЭВМ

Для цитирования: Лабинский А.Ю. Децентрализованное хранение информации // Надзорная деятельность и судебная экспертиза в системе безопасности. 2025. № 1. С. 46–50. DOI: 10.61260/2304-0130-2025-1-46-50.

Введение

Централизованная база данных предполагает её размещение в некотором узле сети. Такая архитектура отличается простотой обслуживания, но не обеспечивает необходимого уровня живучести и своевременного предоставления информационных услуг. Альтернативой централизации является распределение базы данных в сети, в результате чего каждый ее фрагмент располагается в определенном узле, который способен обеспечить наиболее эффективное использование данных [1, 2].

Распределенные базы данных (РБД) могут иметь различную архитектуру, обеспечивающую децентрализованное хранение данных. В данной статье рассматривается такая архитектура РБД, при которой весь массив данных хранится в виде непрерывной последовательности блоков данных, представляющих собой связный список. Связь между блоками данных поддерживается тем, что каждый блок содержит свою хэш-сумму и хэш-сумму предыдущего блока.

Хэш-сумма представляет собой определенную последовательность символов, которая всегда одинакова для определенного набора данных. Для одинаковых данных хэш-сумма равнозначна, что позволяет проверять целостность файлов, содержащих информацию, и находить ошибки при передаче данных. Хэш-сумма определяется с помощью специального алгоритма хэширования данных, который содержит хэш-функцию. Хэш-функция преобразует данные любого размера в строку фиксированной длины. В криптографии хэш-сумма используется как подпись данных (подпись сообщения) [3].

Так как впервые децентрализованное хранение данных было реализовано в виде РБД в системе «Биткоин», то такая база данных (блокчейн, англ. *blockchain* – цепочка связанных блоков) отождествляется со списком (реестром) транзакций (группы операций в базах данных) в различных криптовалютах. В 2008 г. появившаяся система «Биткоин» впервые реализовала децентрализованное хранение информации с использованием технологии блокчейн. В системе «Биткоин» децентрализованная база данных обеспечивает хранение всех тразакций с криптовалютой [4–6].

В настоящее время блокчейн-технологии используются при выполнении финансовых операций, идентификации пользователей для доступа к распределенным в компьютерной сети данным, разработке технологий кибербезопасности. Поэтому на использование блокчейн-технологий обращают внимание многие банковские учреждения и государственные организации [7].

Сформулируем постановку задачи, результаты решения которой представлены в данной статье. Нужно произвести обзор особенностей и возможностей децентрализованного хранения информации с помощью технологии блокчейн.

Новизна исследования, отражающая личный вклад автора, заключается в разработке алгоритма подсчета контрольной суммы CRC-32 (хэш-суммы), используемой для обеспечения связи между блоками данных в РБД, и консольной программы CRC32, реализующей данный алгоритм.

Проблемы блокчейн-технологии распределенных баз данных

Существует ряд проблем, затрудняющих использование блокчейн-технологий, среди которых существенными являются следующие [8–9]:

– в процессе использования наблюдается постоянный рост размеров файлов блокчейна;

– существуют ограничения на пропускную способность каналов связи между узлами сети распределенной базы блокчейна;

– существуют ограничения производительности блокчейна.

Последнее ограничение связано с тем, что в процессе работы необходимо определенное взаимодействие узлов блокчейна с целью достижения согласия о правильности информации, записываемой в очередной блок цепочки данных.

В настоящее время существует три основных типа блокчейнов: публичные, частные и консорциумные.

Публичные блокчейны общедоступны и поддерживают анонимность пользователей. Они децентрализованы и не имеют администратора. Большинство криптовалют используют публичные блокчейны.

В частных блокчейнах существует администратор, который обладает правом записи информации в блоки РБД. Здесь информация без задержки попадает в блоки данных, так как отпадает необходимость в достижении согласия о правильности информации, записываемой в очередной блок цепочки данных. Это повышает скорость работы сети. Доступ к одному виду информации может быть общим, а к другому – ограниченным.

В консорциумных блокчейнах достижение согласия о правильности информации, записываемой в очередной блок цепочки данных, происходит с участием нескольких заранее определенных узлов сети. Эти блокчейны считаются частично децентрализованными.

Применение блокчейн-технологии

Помимо области криптовалют повышенный интерес к блокчейн-технологии проявляет финансовый сектор. Компания для создания специальной платформы снабжения торговли различными товарами, от нефти до пшеницы, была основана 15 международными корпорациями [10–11].

О планах использования блокчейн-технологии заявили платежные системы VISA, Mastercard, Unionplay, SWIFT [12].

В России к блокчейн-технологии проявляют интерес банки ВТБ и Сбербанк. В 2017 г. Альфа-банк запустил блокчейн-платформу для автоматизации торговых операций. В 2021 г. в законодательство России было внесено понятие «Цифровые финансовые активы».

В 2022 г. Центральный банк Индии начал использовать блокчейн-технологии для осуществления денежных переводов за рубеж.

Блокчейн-технологии стали активно применять для удостоверения личности. Финляндия использует блокчейн-технологии для идентификации беженцев. В отдельных странах применяют блокчейн-систему электронного гражданства. В Бразилии работает система удостоверения личности с использованием блокчейн-технологии.

Технология блокчейн может использоваться для проведения онлайн-голосования. По данным 2020 г., в число отраслей экономики России, применяющих блокчейн-технологии, входят: энергетика, добывающая и обрабатывающая промышленность, финансы и логистика.

Циклический избыточный код

Циклический избыточный код (Cyclic Redundancy Check или CRC) это алгоритм нахождения контрольной суммы, используемой для проверки целостности данных. На практике реализация циклического избыточного кода происходит в виде хэш-функции [3].

Контрольная сумма представляет собой некоторое число, рассчитанное по определенному алгоритму на основе входных данных (текстовых сообщений).

Алгоритм CRC основан на свойствах деления с остатком двоичных многочленов. Значение CRC (контрольная сумма) является остатком от деления многочлена, полученного на основе входных данных, на фиксированный порождающий многочлен [3].

Входные данные разбиваются на блоки. Если размер блока равен одному биту, то использующий такой блок алгоритм нахождения контрольной суммы называется CRC-1, если размер блока равен байту (8 бит), то это CRC-8, если это 2 байта (16 бит) – это CRC-16, если 4 байта (32 бита) – это CRC-32.

Реализация алгоритма подсчета контрольной суммы

Алгоритм подсчета контрольной суммы (хэш-суммы) CRC-32 был реализован в виде консольной программы для электронно-вычислительных машин (ЭВМ). Блок-схема алгоритма CRC-32 программы для ЭВМ CRC32 представлена на рис. 1.

Рис. 1. **Блок-схема алгоритма программы определения хэш-суммы**

Окно консольной программы для ЭВМ CRC32, реализующей алгоритм подсчета хэш-суммы CRC-32, представлено на рис. 2.

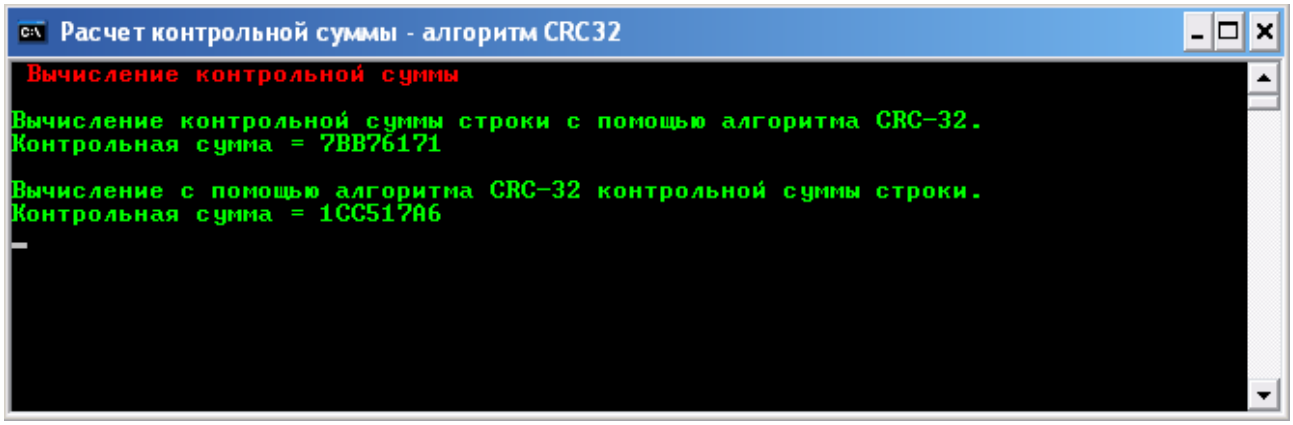

Рис. 2. **Окно консольной программы определения хэш-суммы**

В окне программы CRC32 представлен результат подсчета контрольной суммы (хэш-суммы) для двух строк текста: первая строка «Вычисление контрольной суммы строки с помощью алгоритма CRC-32» – контрольная сумма 7BB76171 и вторая строка «Вычисление с помощью алгоритма CRC-32 контрольной суммы строки» – контрольная сумма 1CC517A6. Перестановка местами нескольких слов привела к изменению контрольной суммы.

Вывод

Последние несколько лет блокчейн-технология в России применяется в различных отраслях энергетики, экономики, добывающей и обрабатывающей промышленности, финансовом и логистическом секторх, что обосновывает актуальность темы статьи.

В настоящее время для децентрализованного хранения данных активно используются РБД, основанные на применении блокчейн-технологии. Архитектура рассматриваемой РБД предусматривает хранение массива данных в виде непрерывной последовательности блоков данных, представляющих собой связный список. Связь между блоками данных поддерживается тем, что каждый блок содержит свою хэш-сумму и хэш-сумму предыдущего блока.

В качестве примера расчета хэш-суммы представлены разработанные автором алгоритм CRC-32 и консольная программа для ЭВМ.

Список источников

1. Иванов А.Ю. Мобильные распределенные базы данных автоматизированных информационно-управляющих систем МЧС России: монография. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2008. 152 с.

2. Равал С. Децентрализованные приложения. Технология Blockchain в действии. СПб.: Питер, 2017. 240 с.

3. Уоррен Г.С. Алгоритмические трюки для программистов. М.: Вильямс, 2007. 288 с.

4. Генкин А.С., Михеев А.А. Блокчейн. Как это работает и что ждет нас завтра. М.: Альпина Паблишер, 2017. 592 с.

5. Генкин А.С., Михеев А.А. Блокчейн для всех. Как работают криптовалюты и другие новые финансовые технологии. М.: Альпина Паблишер, 2023. 588 с.

6. Лелу Л. Блокчейн от А до Я. Все о технологии десятилетия. М.: Эксмо, 2018. 256 с.

7. Могайар У., Бутерин В. Блокчейн для бизнеса. М.: Эксмо, 2017. 224 с.

8. Свон М. Блокчейн: схема новой экономики. М.: Олимп-бизнес, 2017. 240 с.

9. Табернакулов А., Койфманн Я. Блокчейн на практике. М.: Альпина Паблишер, 2019. 264 с.

10. Тапскотт А., Тапскотт Д. Технология блокчейн – то, что движет финансовой революцией сегодня. М.: Эксмо, 2017. 448 с.

11. Haber S., Stornetta W. Blockchain // Journal of cryptography. 2021. Vol. 3. P. 99–111.

12. Nakamoto S. Bitcoin: a per-to-per electronic cash system // Journal of Cryptography. 2019. Vol. 5. P. 37–45.

Информация о статье: статья поступила в редакцию: 02.02.2025; принята к публикации: 03.03.2025

Информация об авторах:

Лабинский Александр Юрьевич, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат технических наук, доцент, e-mail: labinskyi.a@igps.ru, https://orcid.org/0000-0001-2735-4189, SPIN-код: 8338-4230