МОДЕЛЬ БЛОКЧЕЙН-СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ПРОЗРАЧНОСТИ И ВЕРИФИЦИРУЕМОСТИ ДАННЫХ

Федорченко Т.Е.,
студент 2 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Ермоченко С.А., канд. физ.-мат. наук, доцент

Современные системы хранения данных активно используют ограничение доступа для защиты конфиденциальной информации – от медицинских записей до финансовых транзакций. Однако в сценариях, где требуется публичная проверка целостности данных и отслеживание их истории (например, цифровые архивы, цепочки поставок, юридические документы), это создаёт парадоксальную ситуацию: строгий контроль доступа, обеспечивающий безопасность, одновременно препятствует реализации механизмов публичной верификации целостности и отслеживаемости данных [1].

Для решения этой проблемы предлагается модель хранения данных, основанная на принципах блокчейн-технологии. Её ключевая задача – обеспечить:

- *неизменность данных* – защиту от редактирования или удаления информации после записи;
- *прозрачный аудит* – возможность проверки целостности и истории изменений без раскрытия конфиденциальных деталей;
- *децентрализованную верификацию* – механизмы, позволяющие пользователям самостоятельно убеждаться в подлинности данных.

Целью данного исследования является анализ технологии блокчейн для разработки на её основе децентрализованной системы хранения данных, которую можно легко адаптировать под различные предметные области.

Материал и методы. Использовался метод математического моделирования, а также общенаучные методы анализа и синтеза, дедукции и индукции.

Результаты и их обсуждение. Блокчейн представляет собой распределённую базу данных, организованную в виде последовательности взаимосвязанных блоков.

Рисунок 1 – Цепочка блоков блокчейна

Каждый блок содержит:

- *Данные:* время создания блока, его порядковый номер, хранимые данные;
- *Криптографический хеш предыдущего блока* [2], подтверждающий целостность цепочки;
- *Собственный хеш*, вычисляемый на основе его содержимого (включая данные и хеш предыдущего блока).

Для обеспечения децентрализации и устойчивости к изменениям, полные копии цепочки блоков должны храниться на множестве независимых узлов сети. Это исключает единую точку отказа и затрудняет фальсификацию данных, так как злоумышленнику потребуется изменить все копии одновременно. [3]

Ключевым элементом работы блокчейна является консенсусный механизм – алгоритм, гарантирующий согласованность данных между узлами. Например, в модели Proof of Work (PoW) добавление нового блока требует решения криптографической задачи, которая:

– имеет *высокую вычислительную сложность;*
– *легко проверяется* другими участниками сети.

Такая модель консенсуса служит защитой от спама и атак, так как злонамеренные действия становятся экономически невыгодными. [4]

На основе технологии блокчейн можно создать децентрализованную систему, гарантирующую целостность данных и прозрачность их изменений.

Рисунок 2 – Схема работы децентрализированной системы блокчейна

Преимущества:

– *Неизменяемость данных* (криптографическая защита от фальсификации),
– *Децентрализация* (отсутствие единого контроля),
– *Прозрачность* (доступность истории операций для всех участников),
– *Устойчивость к атакам* (за счёт распределённого консенсуса),
– *Автоматизация* (исполнение правил через смарт-контракты).

Ограничения:

– *Низкая масштабируемость* (ограничение скорости обработки транзакций),
– *Высокая ресурсоёмкость* (энергозатраты в PoW-сетях),
– *Ограниченный объём данных* (непригодность для хранения больших файлов, например, медиаконтента)**.**

Заключение. Таким образом, в работе рассмотрены возможности технологии блокчейн. Как видно, реализация консенсусного механизма не зависит от структуры или характера данных, хранящихся в области данных, что позволяет хранить данные самых различных предметных областей. Однако, из-за указанных ограничений, в дальнейшем система хранения будет разрабатываться для хранения сравнительно небольшого объёма данных со средней скоростью их прироста. Такая система может применять для хранения некоторых документов, например, дипломов об образовании, или выдаваемых сертификатах и т.п.

1. Коннолли Т., Бегг К. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. – 3-е изд. – М.: Вильямс, 2003. – 1436 с.

2. Криптографические методы: метод. рекомендации / [сост. Е.А. Витько]; М-во образования Республики Беларусь, Учреждение образования "Витебский государственный университет имени П. М. Машерова", Каф. информатики и информационных технологий. – Витебск: ВГУ имени П. М. Машерова, 2019. – С. 27 URL: https://rep.vsu.by/handle/123456789/19133 (дата обращения 13.03.2024)

3. Franco P. The Blockchain // Understanding Bitcoin: Cryptography, Engineering and Economics. – Hoboken, NJ: John Wiley & Sons, 2014. – 288 p.

4. Institute of Electrical and Electronics Engineers, Computer Society. IEEE Computer Architecture Letters / Institute of Electrical and Electronics Engineers. – 2002. – URL: http://www.computer.org/csdl/letters/ca/index.html.