МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЛОГИСТИЧЕСКОЙ БЛОКЧЕЙН СИСТЕМЫ

С. А. Корчагин, Д. А. Шелудяков, Д. В. Терин

Саратовский государственный технический университет им. Ю. А. Гагарина, Россия
E-mail: korchaginser@gmail.com, dimka.ice@yandex.ru, terinden@mail.ru

Рассмотрены примеры практического применения технологии блокчейн в логистических решениях. Разработана математическая модель логистической блокчейн-системы на основе алгоритма ассиметричного шифрования данных RSA, а также модель обмена данными между пользователями. Установлены основные уязвимости таких систем и даны рекомендации по совершенствованию обеспечения безопасности логистических блокчейн систем. Проведено сравнение традиционных логистических систем с решениями на основе технологии блокчейн.

MATHEMATICAL MODELING OF LOGISTIC BLOCKCHAIN SYSTEM

S. A. Korchagin, D. A. Sheludyakov, D. V. Terin

Examples of the practical application of blockchain technology in logistics solutions are considered. A mathematical model of the logistic blockchain system based on the asymmetric RSA data encryption algorithm is developed, as well as a model for exchanging data between users. The main vulnerabilities of such systems are identified and recommendations are given for improving the security of logistics blockchain systems. A comparison is made of traditional logistics systems with solutions based on blockchain technology.

В настоящее время технологии оказывают большое влияние на экономику, в частности на взаимодействие участников рынка. Традиционные представления о базовых экономических понятиях, таких как торговля, собственность, взаимодействие игроков рынка трансформируются в значительной мере [1]. Изменение бизнес-моделей приводит к потребности в технологии, которая сможет обеспечить прозрачность и защищенность всех связанных процессов. Одной из таких технологий является блокчейн - способ хранения информации, при котором данные записываются в блоки в распределительном реестре [2]. Анализ блокчейн-систем [3-5] позволяет выделить основные свойства блокчейна: наличие базы данных; использование шифрованных методов идентификации пользователей; распределенность между пользователями; свободная регистрация и последующий свободный доступ к функционалу; защищенный механизм консенсуса.

Основой новых проектов, построенных на блокчейне, по заявлению разработчиков являются открытость, защищенность, безопасность [6].

Одной из задач защиты информации является обеспечение достоверности данных. В настоящем исследовании мы рассматриваем алгоритм ассиметричного шифрования RSA. Данный метод шифрования активно используется в логи-

стических блокчейн системах, например [7-9]. Математическая модель будет иметь вид:

$$n = b \cdot c \quad (1)$$

$$\phi(n) = (b-1)(c-1) \quad (2)$$

$$c \cdot e \bmod \phi(n) = 1 \quad (3)$$

$$d = m^e \bmod n \quad (4)$$

$$m = d^c \bmod n \quad (5)$$

где *b, c* - простые числа, *n* - модуль для открытого и закрытого ключа, $\phi(n)$ - функция Эйлера. После выбора простых чисел выбирается целое число e (открытая экспонента) от 1 до $\phi(n)$. Далее находится число *c*, отвечающее формуле (3). Таким образом, формируется приватный ключ {*c,n*} и публичный ключ {*d,n*} при помощи, которых производится шифрование (4) и дешифрование данных (5).

Цифровые подписи в блокчейне основаны на методах криптографии с открытым ключом. Используются два ключа: закрытый ключ — используется для формирования цифровых подписей и хранится в секрет, открытый ключ — необходим для проверки электронной подписи. Открытый ключ вычисляется на основе закрытого ключа, а вот обратное преобразование требует большого объема вычислений.

При попытке подобрать закрытый ключ придется перебрать 2^N комбинаций, где N - длина ключа. Подбор ключа брут-форсом [10] даже на самых современных высокопроизводительных кластерах займет продолжительное время. Так, например, при длине ключа в 256 бит и скорости подбора паролей 1024 в секунду потребуется 1,23e + 67 лет. Таким образом, рассмотренный метод шифрования, применяемый в логистических блокчейн-системах, имеет высокий уровень защищенности. Угрозой могут быть квантовые компьютеры, обладающие высокими производительными мощностями по сравнению с традиционными компьютерами, однако, использование дополнительных методов защиты (например, блокирующие алгоритмы) решают эту проблему.

Еще одной важной задачей защиты информации, затрагивающей, логистические блокчейн-решения является обеспечение доверия пользователей [11]. Модель, обеспечивающая доверие пользователей будет выглядеть следующим образом (см. рисунок). Все транзакции между всеми сторонами в такой сети дезинтегрированы и децентрализованы на глобальном уровне.

Мы провели сравнение технологии блокчейн и традиционной технологий хранения данных в логистических системах, результаты отражены в таблице.

Модель обмена данными между пользователями

Сравнение технологии блокчейн и традиционной технологий хранения данных в логистических системах

Характеристика	Технология блокчейн	Традиционные технологии
Владение данными	Поддерживание посредством криптографических ключей и собственных криптографических алгоритмов	Центральный орган управления
Конфиденциальность и безопасность	Криптографическая аутентификация	Настройка каждой строки на основе принудительного исполнения из центрального органа
Доверие	Через неизменяемые записи	Через центральный орган
Качество данных	Неизменяемая запись с автоматическим разрешением конфликтов посредством консенсуса по транзакциям	Для сложных процессов разрешения конфликтов требуется ручное вмешательство
Действительность базы данных	Непрерывный поток	Предоставляется только для отдельных экземпляров во времени
Распространение данных	Быстрое распространение по всем сетевым заметкам	Посредством пользовательских процессов синхронизации
Надежность и доступность	Одноранговая сеть для распределенной репликации данных по всем узлам	Потенциальная единственная точка отказа
Хранимые процедуры	Умные контракты	Недоступно
Создание транзакции	Доступно для всех разрешенных сторон	Управление через центральный орган

Таким образом, использование блокчейн в логистических системах решает проблемы, характерные для традиционных систем баз данных. Блокчейн

обеспечивает безопасное пространство для хранения всех записей. Поскольку данные децентрализованы, плавное функционирование системы не зависит от любого конкретного поставщика облачных услуг. Поскольку в цепочке блоков технология не позволяет менять данные после их записи, они не могут быть изменены владельцами для личных целей. Математическое моделирование подтверждает, часть полученных выводов, в частности касающихся достоверности получаемой информации и её защищенности.

СПИСОК ЛИТЕРАТУРЫ

1. *Peters G. W., Efstathios P.* Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money // Banking Beyond Banks and Money. Springer, Cham. 2016. P. 239-278.

2. *Ekblaw A., et al.* A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data // Proceedings of IEEE Open & Big Data Conference. 2016.

3. *Samaniego M., Ralph D.* Using blockchain to push software-defined IoT components onto edge hosts // Proceedings of the International Conference on Big Data and Advanced Wireless Technologies. ACM. 2016.

4. *Muneeb A., et al.* Blockstack : A Global Naming and Storage System Secured by Blockchains // USENIX Annual Technical Conference. 2016.

5. *Яковлева Е. Ю., Сергеев И. В.* Обзор технологии блокчейн в качестве инструмента таможенного администрирования // Молодой ученый. 2017. № 20. С.301-304. [Электронный ресурс]. URL: https://moluch.ru/archive/154/43535/ (дата обращения: 16.10.2018).

6. *Zyskind G., Nathan O.* Decentralizing privacy : Using blockchain to protect personal data // Security and Privacy Workshops (SPW). 2015.

7. *Vorick D., Champine L.* Sia : simple decentralized storage. Security and Privacy Workshops (SPW). 2014.

8. *Christidis K., Devetsikiotis M.* Blockchains and smart contracts for the internet of things // Ieee Access. 2016. Т. 4. С. 2292-2303.

9. *Kosba A. et al.* Hawk: The blockchain model of cryptography and privacy-preserving smart contracts // 2016 IEEE symposium on security and privacy (SP). IEEE. 2016. С. 839-858.

10. *Воронов М. П., Часовских В. П.* Blockchain–основные понятия и роль в цифровой экономике // Современные проблемы науки и образования. 2017. №. 9-1. С. 30-35.

11. *Соколова Т. Н., Сыксин В. В.* Управление децентрализованными системами с помощью технологии blockchain // Информационная безопасность регионов. 2017. №. 1 (26).