DOI 10.37882/2223-2966.2025.07.32

АНАЛИТИЧЕСКАЯ ОЦЕНКА ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМ В КАЧЕСТВЕ АЛЬТЕРНАТИВЫ ДЛЯ ОРГАНИЗАЦИИ ХРАНИЛИЩ ДАННЫХ

ANALYTICAL ASSESSMENT OF DECENTRALIZED SYSTEMS AS AN ALTERNATIVE FOR DATA STORAGE ORGANIZATION

S. Tarasenko
Yu. Koroleva

Summary. This study conducts a comprehensive analysis of the prospects and limitations associated with the application of blockchain technology as an alternative approach to data storage compared to traditional methods. The technical features of blockchain are examined, its suitability for various types of data is analyzed, and potential areas of application are identified. The aim of this research is to provide an objective assessment of the advantages and disadvantages of blockchain technology as an alternative solution for data storage, taking into account contemporary requirements and challenges in information security and data management.

The study is conducted considering the current technical and theoretical aspects of blockchain technology, including its decentralized nature, consensus mechanisms, and cryptographic principles. An analysis of the possibilities for effectively applying decentralized data storage is provided.

The research text presents recommendations for the optimal selection of data storage methods depending on specific scenarios and usage goals, considering the limitations inherent in decentralized data storage. The obtained results can serve as a basis for making informed decisions in the field of data storage and management, as well as for developing strategies for implementing blockchain technology in modern information systems.

Keywords: decentralization, data storage, smart contracts, blockchain, information security.

Тарасенко Сергей Сергеевич
кандидат технических наук, Академия ФСО России
Dor7la96@mail.ru
Королева Юлия Евгеньевна
независимый исследователь, г. Орёл
Julkor3@yandex.ru

Аннотация. В данном исследовании проводится комплексный анализ перспектив и ограничений, связанных с применением технологии блокчейн в качестве альтернативного подхода к хранению данных по сравнению с традиционными методами. Рассмотрены технические особенности блокчейна, проведен анализ его пригодности для разнообразных типов данных и обозначены потенциальные области применения. Целью данного исследования является предоставление объективной оценки преимуществ и недостатков технологии блокчейн в качестве альтернативного решения для хранения данных с учетом современных требований и вызовов информационной безопасности и управления данными.

Исследование осуществлено с учетом актуальных технических и теоретических аспектов технологии блокчейн, включая ее децентрализованную природу, механизмы консенсуса и криптографические принципы. Проведен анализ возможностей эффективного применения децентрализованных хранилищ данных.

В тексте исследования представлены рекомендации по оптимальному выбору методов хранения данных в зависимости от конкретных сценариев и целей использования с учетом ограничений, присущих децентрализованным хранилищам данных. Полученные результаты могут служить основой для принятия решений в области хранения и управления данными, а также для разработки стратегий внедрения технологии блокчейн в современные информационные системы.

Ключевые слова: децентрализация, хранилище данных, смарт-контракт, блокчейн, защита информации.

Введение

В современной информационной эпохе, сконцентрированной на передаче, хранении и обработке данных, существует непрерывная потребность в эффективных и безопасных методах сохранения информации. Вопросы, связанные с обеспечением конфиденциальности, целостности и доступности данных, являются приоритетными для организаций и индивидуальных пользователей. Традиционные подходы к хранению данных, такие как облачные и локальные хранилища, несмотря на свою широкую распространенность, имеют ряд существенных ограничений и недостатков.

Облачные хранилища данных обладают такими характеристиками как масштабируемость и удобство доступа к данным из любой точки мира. Однако, они подвержены риску утечки конфиденциальной информации и зависимости от централизованных поставщиков услуг, что может привести к потере контроля над данными и уязвимостям в безопасности.

Локальные хранилища данных, с другой стороны, могут обеспечить более высокий уровень контроля и безопасности, но они ограничены в масштабируемости и доступности, особенно при необходимости удаленного доступа к данным.

С учетом данных ограничений в поиске более эффективных и безопасных методов хранения данных, технология блокчейн [1] выделяется как перспективная альтернатива. Блокчейн представляет собой децентрализованную и распределенную систему хранения данных, обеспечивающую высокий уровень безопасности и стойкость к несанкционированной модификации хранящихся данных.

Преимущества и недостатки технологии блокчейн

Преимущества:

1) *Повышенная защищенность от несанкционированного изменения данных, размещенных блокчейне.* В блокчейне каждый блок данных связан с предыдущими блоками с использованием хеш-функций. Это создает цепочку блоков, где каждый блок содержит уникальный идентификатор, зависящий от содержимого предыдущего блока. Если даже небольшое изменение в данных произойдет в предыдущем блоке, это приведет к изменению хеш-кода, что автоматически приведет к изменению хеш-кодов всех последующих блоков в цепочке. Содержимое блока составляют транзакции пользователей, подписанные цифровыми подписями с использованием приватных ключей пользователей. Таким образом, цифровые подписи и хеширование делают нереализуемым на практике изменение данных в блокчейне без возможности обнаружения.
2) *Децентрализация*. В отличие от централизованных систем, где данные хранятся и управляются одним центральным органом, в блокчейне данные распределены между множеством узлов в сети. Эти узлы синхронизированы между собой, и каждый узел содержит полную копию всей цепочки блоков (базы данных). Это делает блокчейн устойчивым к атакам и изменениям, так как атакующему потребуется изменить данные на всех узлах сети одновременно, что в больших и независимых сетях практически невозможно.
3) *Дороговизна и нецелесообразность атак на подобные системы*. Стоимость и неоправданность атак на подобные системы проявляются в контексте блокчейна за счет использования консенсусных механизмов, которые регулируют изменения в базе данных между узлами сети. Разнообразные алгоритмы консенсуса, такие как *Proof of Work* (*PoW*) [2], *Proof of Stake* (*PoS*) [3] и другие, обеспечивают достижение единства среди узлов относительно приемлемых данных для добавления в блокчейн, исключая нежелательные изменения. Это устраняет возможные атаки или попытки внести изменения в данные путем обеспечения консенсуса [4] среди всех участников сети. Необходимость контроля большинства узлов в сети для успешной атаки [5] подтверждает, что стоимость таких атак для масштабных блокчейн-сетей может быть высока и обнаружена остальными участниками сети, а также наблюдателями или разработчиками блокчейн-проекта. После выявления атаки «честная» часть сообщества пользователей и разработчики могут создать копию сети с состоянием, которое было в сети до атаки, тогда как копия с навязанными атакующими данными будет считаться недействительной. Поскольку ценность блокчейн-системы определяется ее децентрализованным характером и доверием пользователей, то скомпрометированная сеть и данные в ней перестают быть ценными для сообщества. Следовательно, даже в случае успешной атаки на блокчейн-систему она будет обнаружена и, с применением описанного выше механизма, возвращена к состоянию, предшествовавшему атаке, что делает проведение таких атак (с учетом их дороговизны) нецелесообразным.
4) *Резервирование данных*. Автоматическое резервирование данных в блокчейне обеспечивается за счет хранения информации на распределенном множестве узлов сети, что исключает необходимость в специальных процедурах и дополнительных ресурсах. Этот механизм гарантирует сохранность данных даже при выходе из сети отдельных участников, не приводя к их потере или недоступности.
5) *Отсутствие необходимости в backend-сервере*. Для определенных задач, веб-приложения и децентрализованные приложения (*dApp*) [6] могут обходиться без необходимости использования *backend*-сервера, так как блокчейн может выступать в роли такого сервера, обеспечивая возможность обработки данных и выполнения логики приложения через его смарт-контракты. Это также освобождает от необходимости траты ресурсов на содержание инфраструктуры сервера и обеспечение аутентифицированного доступа пользователей, что способствует упрощению разработки и экономии средств.
6) *Гарантия выполнения условий и операций, определенных в смарт-контрактах*. Обеспечение выполнения условий и операций, определенных в смарт-контрактах [7], обеспечивается автоматически и надежно благодаря принципам децентрализации и непротиворечивости в блокчейне. Смарт-контракты представляют собой программные коды, которые хранятся и исполняются в блокчейне, и обеспечивают автоматическое выполнение договоренностей между сторонами без необходимости доверия к третьей стороне. Этот механизм гарантирует надежность и прозрачность исполнения условий смарт-контракта, исключая возможность манипуляций или несоблюдения соглашений со стороны участников.

Недостатки:

1) *Низкая производительность блокчейна* является значимым ограничением, присущим данной технологии, и обусловлена рядом факторов. Прежде всего, увеличение количества транзакций в сети блокчейна приводит к увеличению времени обработки и подтверждения каждой транзакции. Это происходит из-за необходимости достижения консенсуса между всеми участниками сети, что требует временных затрат. *Данный недостаток накладывает ограничение на реализацию на базе технологии блокчейн хранилища информации, предоставляющего инструментарий для изменения/добавления данных в хранилище в режиме реального времени.*
2) *Рост количества информации, хранимой в блокчейне*. Увеличение объема данных в блокчейне, без возможности удаления или изменения сохраненных в нем данных, является характерной особенностью данной технологии. Вследствие этого, увеличение объема данных в блокчейне приводит к накоплению информации в цепочке блоков, сохраняя каждое состояние системы с момента ее создания. Однако, при этом возникают проблемы с масштабируемостью и эффективным управлением большим объемом данных, так как каждый узел в сети должен хранить полную копию блокчейна. *Данный недостаток указывает на нецелесообразность хранения в блокчейне больших объемов данных.*
3) *Дублирование информации на всех узлах сети, в сочетании с невозможностью удаления или изменения сохраненных в сети данных, создает потенциальную угрозу безопасности информации*. При сохранении данных в блокчейне они остаются неизменными и доступными на всех узлах сети, что может привести к серьезным последствиям в случае утечки конфиденциальной информации или ошибочного внесения неправильных данных. *Данный недостаток указывает на необходимость использования шифрования информации перед ее размещением в блокчейне с помощью стойких криптографических методов, способных обеспечить конфиденциальность сведений в долгосрочной перспективе*.
4) *Несовместимость различных блокчейн-сетей* представляет собой значительное ограничение для развития блокчейн-технологий и обеспечения взаимодействия между смарт-контрактами разных сетей. Это связано с тем, что различные блокчейны могут иметь разные протоколы консенсуса, форматы данных, архитектуру смарт-контрактов и другие технические особенности, что делает их несовместимыми между собой. *Данный недостаток указывает на трудоемкость и нецелесообразность (без веских причин) создания хранилищ информации, задействующих несколько различных блокчейн-сетей*.
5) *Слабая связь с реальным миром*, также известная как проблема «оракулов» [8], является одним из ограничений блокчейн-технологии. Она связана с тем, что большинство блокчейн-сетей не имеют возможности напрямую взаимодействовать с внешними данными или событиями, происходящими в реальном мире. Оракулы — это сторонние сервисы или узлы, которые предоставляют информацию о внешних событиях или данных в блокчейн. Они выполняют функцию по передаче внешних данных в блокчейн, чтобы они могли быть использованы в смарт-контрактах или других децентрализованных приложениях.

Однако *использование оракулов вводит некоторые риски*, включая:

a) *Недостаточная децентрализация*: оракулы могут быть централизованными или подвержены взлому, что может привести к манипуляциям или фальсификации внешних данных, поступающих в блокчейн.
b) *Односторонняя доверенность*: децентрализованные приложения могут полагаться только на те данные, которые им предоставляют оракулы. Это создает риск, что информация, поступающая извне, может быть неточной или недостоверной.
c) *Сложности интеграции*: интеграция оракулов с блокчейн-сетями может быть сложной и требовать дополнительных ресурсов и усилий для обеспечения безопасности и надежности передачи данных.

Данный недостаток указывает на недопустимость применения оракулов для обеспечения функционала хранилища информации в блокчейн-системе, ответственного за конфиденциальность, целостность и доступность пользовательских данных.

6) *За действия в сети блокчейна, за исключением чтения данных, предусмотрено взимание платы*. Данная плата, называемая «комиссия» или «*gas*» [9], представляет собой форму оплаты, которую пользователи сети должны уплатить за выполнение определенных операций или транзакций в блокчейне.

В сети *Ethereum* [10] комиссия взимается за выполнение функций смарт-контрактов или передачу токенов между пользователями. Размер комиссии зависит от ресурсов, требуемых для выполнения операции, таких как объем вычислений, необходимый для выполнения смарт-контракта, или размер данных, передаваемых в транзакции.

Данные платежи выполняют важную роль в поддержании безопасности и эффективности работы блокчейн-сети, так как они обеспечивают мотивацию для участников сети, таких как «майнеры» (для *PoW*) или «валидаторы» (для *PoS*) продолжать свою деятельность. Кроме того, плата комиссии служит средством защиты от *DDoS*-атак [11], так как высокие комиссии делают экономически невыгодным отправку большого количества ненужных транзакций. Это помогает сохранять работоспособность сети и обеспечивает эффективное использование ее ресурсов, способствуя созданию устойчивой и надежной блокчейн-экосистемы. *Данный недостаток указывает на экономическую нецелесообразность хранения больших объемов данных, не имеющих критического значения, а также необходимость декомпозировать и структурировать хранимую информацию, чтобы при изменении незначительной части данных не требовалось изменение большого объема информации, размещенной в блокчейне*. Это создает необходимость разработки специализированных методов хранения и обработки зашифрованной информации, учитывающих как различные аспекты защиты от угроз безопасности информации, размещенной в блокчейн-сети, так и экономическую эффективность операций с данной информацией.

Сравнительный анализ локальных, облачных и децентрализованных хранилищ данных

Достоинства локальных хранилищ данных.

1. Высокий уровень контроля и безопасности (нет необходимости в доверии внешней организации);
2. Невозможность «отказа в обслуживании» (нет необходимости в доверии внешней организации);
3. Отсутствие платы за обслуживание.

Недостатки локальных хранилищ данных.

1. Отсутствие резервирования + утеря устройства = утеря данных;
2. Отсутствие «синхронизации» между устройствами пользователя.

Достоинства облачных хранилищ данных.

1. Резервирование данных;
2. «Синхронизация» данных между устройствами пользователя.

Недостатки облачных хранилищ данных.

1. Инфраструктура безопасности облачного хранилища, не подлежащая открытому аудиту, может содержать уязвимости;
2. Возможен «отказ в обслуживании», и, как следствие, утеря доступа к данным;
3. Необходимость платы за обслуживание (как за доступ к данным, так и за хранение и/или изменение данных).

Достоинства децентрализованных хранилищ данных.

1. Высокий уровень контроля и безопасности (нет необходимости в доверии внешней организации);
2. Невозможность «отказа в обслуживании» (нет необходимости в доверии внешней организации);
3. Резервирование данных;
4. «Синхронизация» данных между устройствами пользователя.

Недостатки децентрализованных хранилищ данных.

1. Необходимость платы за обслуживание (только за изменение данных).

Таким образом, децентрализованное хранилище данных представляет собой синтез преимуществ локальных и «облачных» подходов к хранению информации, а из недостатков наследует только необходимость платы за обслуживание, связанное с изменением данных.

Области применения

Учитывая перечисленные достоинства и недостатки технологии блокчейн, можно выделить ряд прикладных областей, в которых целесообразно использование децентрализованного хранилища данных:

1) Децентрализованные менеджеры паролей. Авторизационная и аутентификационная информация имеет критическое значение для пользователей и занимает относительно небольшой информационный объем. Также для данной предметной области не требуется поддержка функционирования в режиме реального времени.
2) Децентрализованные хранилища исходных кодов проектов. Именно хранение исходных кодов готовых проектов, изменения в которые будут вноситься только со значимыми обновлениями («релизами» программного обеспечения). Использование блокчейна в качестве распределенной системы управления версиями исходного может быть экономически неэффективным.
3) Децентрализованные хранилища небольших файлов и документов. Это могут быть, например, конфигурационные файлы для информационных систем или внутренняя документация организаций.

Приведенный перечень не является исчерпывающим. Он может быть дополнен и расширен в зависимости от конкретной области и решаемых организацией или индивидуальным пользователем типов задач.

Заключение

Резюмируя вышесказанное, можно сделать следующий вывод. Децентрализованные хранилища данных

представляют собой интеграцию сильных сторон локальных и «облачных» систем хранения информации. Используя преимущества обоих подходов, такие системы обеспечивают повышенную отказоустойчивость, гарантированную доступность, распределенный доступ и прозрачность оперирования с хранимыми данными. Однако для поддержания такой структуры может потребоваться плата за обслуживание, особенно при частых изменениях данных. Эта необходимость обусловлена требованием к согласованию изменений между различными узлами децентрализованной сети, что может привести к дополнительным операционным расходам, что в свою очередь, в совокупности с ограничениями в производительности блокчейн-систем, накладывает определенные ограничения на сферы применения подобных хранилищ, а также указывает на необходимость разработки специальных адаптированных к определенной предметной области способов организации хранения и обработки данных в смарт-контрактах.

ЛИТЕРАТУРА

1. Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. ACM Computing Surveys (CSUR), 52, 1–34. https://doi.org/10.1145/3316481.
2. Gervais, A., Karame, G., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/2976749.2978341.
3. Saleh, F. (2020). Blockchain Without Waste: Proof-of-Stake. Information Systems & Economics eJournal. https://doi.org/10.2139/ssrn.3183935.
4. Zhang, S., & Lee, J. (2020). Analysis of the main consensus protocols of blockchain. ICT Express, 6, 93–97. https://doi.org/10.1016/J.ICTE.2019.08.001.
5. Aponte-Novoa, F., Orozco, A., Villanueva-Polanco, R., & Wightman, P. (2021). The 51 % Attack on Blockchains: A Mining Behavior Study. IEEE Access, PP, 1-1. https://doi.org/10.1109/ACCESS.2021.3119291.
6. Cai, W., Wang, Z., Ernst, J., Hong, Z., Feng, C., & Leung, V. (2018). Decentralized Applications: The Blockchain-Empowered Software System. IEEE Access, 6, 53019–53033. https://doi.org/10.1109/ACCESS.2018.2870644.
7. Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. Telematics Informatics, 35, 2337–2354. https://doi.org/10.1016/J.TELE.2018.10.004.
8. Sheldon, M. (2020). Auditing the Blockchain Oracle Problem. J. Inf. Syst., 35, 121–133. https://doi.org/10.2308/isys-19-049.
9. Koutmos, D. (2023). Network Activity and Ethereum Gas Prices. Journal of Risk and Financial Management. https://doi.org/10.3390/jrfm16100431.
10. Tikhomirov, S. (2017). Ethereum: State of Knowledge and Research Perspectives. 206–221. https://doi.org/10.1007/978-3-319-75650-9_14.
11. Behal, S., Kumar, K., & Sachdeva, M. (2017). Characterizing DDoS attacks and flash events: Review, research gaps and future directions. Comput. Sci. Rev., 25, 101–114. https://doi.org/10.1016/j.cosrev.2017.07.003.

Журнал «Современная наука: актуальные проблемы теории и практики»