Qabul qilindi: 10.07.2024 Chop etildi: 30.08.2024 UDK: 34(045)(575.1)

ПРАВОВЫЕ И ЭТИЧЕСКИЕ ПРОБЛЕМЫ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В ТЕХНОЛОГИИ БЛОКЧЕЙН

Рузимуродов Бехруз Рустамович,
Магистрант Ташкентского государственного юридического университета по специальности «Право государственного управления»

https://orcid.org/0009-0004-4268-5877

behruzterrabite@gmail.com

LEGAL AND ETHICAL ISSUES OF STORING PERSONAL DATA IN BLOCKCHAIN TECHNOLOGY

Ruzimurodov Bekhruz Rustamovich,
Master's student of Tashkent State Law University, specializing in "Law of Public Administration"

BLOKCHEYN TEXNOLOGIYASIDA SHAXSIY MA'LUMOTLARNI SAQLASHNING HUQUQIY VA AXLOQIY MASALALARI

Ruzimurodov Behro'z Rustamovich,
Toshkent davlat yuridik universiteti "Davlat boshqaruv huquqi'' yo'nalishi magistranti

Annotatsiya: Maqola GDPR va CCPA talablarini hisobga olgan holda, blokcheyn texnologiyalaridan foydalangan holda shaxsiy ma'lumotlarni saqlashning huquqiy va axloqiy jihatlarini tahlil qiladi. Sifat tahlili va huquqiy ekspertiza asosida olib borilgan tadqiqot, blokcheynning o'zgarmasligi ushbu reglamentlarda belgilangan ma'lumotlarni o'chirish huquqi va iste'molchilar nazorati bilan zid ekanligini ko'rsatadi. Gibrid modellar va maxfiylikni oshiruvchi texnologiyalar kabi mumkin bo'lgan yechimlar hamda maxfiylik, rozilik va ma'lumotlarga egalik qilish kabi axloqiy masalalar muhokama qilinadi.

Kalit so'zlar: Blokcheyn texnologiyasi, shaxsiy ma'lumotlar, GDPR, CCPA, ma'lumotlar maxfiyligi, qonuniy muvofiqlik, axloqiy mulohazalar, o'zgarmaslik, ma'lumotlarni himoya qilish, ma'lumotlarni saqlashning gibrid modellari.

Аннотация: Статья анализирует правовые и этические аспекты хранения персональных данных с использованием блокчейн-технологий, учитывая требования GDPR и CCPA. Исследование, основанное на качественном анализе и юридической экспертизе, выявляет, что неизменяемость блокчейна противоречит праву на удаление данных и потребительскому контролю, предусмотренным этими регламентами. Обсуждаются возможные решения, такие как гибридные модели и технологии повышения конфиденциальности, а также этические вопросы конфиденциальности, согласия и владения данными и предлагаются направления для будущих исследований.

Ключевые слова: технология блокчейн, персональные данные, GDPR, CCPA, конфиденциальность данных, соблюдение законодательства, этические соображения, неизменяемость, защита данных, гибридные модели хранения данных.

Abstract: The article analyzes the legal and ethical aspects of storing personal data using blockchain technology, considering the requirements of GDPR and CCPA. The research, based on qualitative analysis and legal expertise, reveals that the immutability of blockchain conflicts with the right to data deletion and consumer control provided by these regulations. Possible solutions, such as hybrid models and privacy-enhancing technologies, as well as ethical issues related to privacy, consent, and data ownership, are discussed.

The need for compliance monitoring and regulation is emphasized. The study acknowledges its limitations and suggests directions for future research.
Keywords: blockchain technology, personal data, GDPR, CCPA, data privacy, legal compliance, ethical considerations, immutability, data protection, hybrid data storage models.

I.Введение. Технология блокчейн, изначально разработанная для цифровой валюты Bitcoin, стала новаторской инновацией с приложениями, выходящими далеко за рамки криптовалют. Блокчейн — это децентрализованная, распределенная система реестра, которая записывает транзакции на многих компьютерах, так что запись не может быть изменена задним числом без изменения всех последующих блоков и консенсуса сети. Присущие этой технологии характеристики прозрачности, безопасности и неизменности делают ее привлекательным решением для различных секторов, включая финансы, управление цепочками поставок, здравоохранение и, в частности, хранение данных.

Особого внимания заслуживает растущее использование блокчейна для хранения персональных данных. Потенциал блокчейна в предоставлении безопасных, защищенных от несанкционированного доступа записей делает его привлекательным вариантом для обработки конфиденциальной информации, такой как личная идентификация, медицинские записи и финансовые данные. Однако децентрализованная и неизменяемая природа блокчейна вызывает серьезные правовые и этические проблемы, особенно в контексте защиты персональных данных и прав на неприкосновенность частной жизни.

С этической точки зрения использование блокчейна для хранения персональных данных выдвигает на первый план вопросы, связанные с конфиденциальностью, согласием и прозрачностью. Постоянный и публичный характер записей блокчейна может привести к непреднамеренному раскрытию персональной информации, что нарушает права лиц на конфиденциальность. Более того, получение подлинного согласия от лиц, чьи данные будут храниться в неизменяемом реестре, является сложной задачей, поскольку они могут не в полной мере понимать долгосрочные последствия такого хранения.

Цель данной статьи — проанализировать правовую и этическую основу хранения персональных данных с использованием технологии блокчейн. В нем будут рассмотрены соответствующие законы и нормативные акты, изучены этические принципы, применимые к хранению данных, и изучены примеры внедрения блокчейна для выявления передовой практики и потенциальных ловушек.

Решение правовых и этических проблем, связанных с хранением персональных данных на основе блокчейна, имеет решающее значение по нескольким причинам. Во-первых, обеспечение соблюдения законов о защите данных имеет важное значение для избежания правовых последствий и финансовых штрафов. Во-вторых, этические методы обработки данных необходимы для поддержания общественного доверия и поддержки технологии блокчейна. Поскольку блокчейн продолжает развиваться и интегрироваться во все большее количество аспектов общества, создание надежной правовой и этической основы будет иметь основополагающее значение для его устойчивого развития.

Используя сложное взаимодействие между технологией, законом и этикой, заинтересованные стороны могут использовать преимущества блокчейна, одновременно защищая персональные данные и отстаивая права личности. Этот анализ будет способствовать текущему дискурсу и предоставит действенные идеи для политиков, разработчиков и организаций, стремящихся ответственно внедрять решения на основе блокчейна.

II. Методы 2.1. План исследования

В этом исследовании используется смешанный метод исследования, сочетающий качественный анализ и юридический обзор для изучения правовой и этической основы хранения персональных данных в технологии блокчейн.

Качественный подход включает в себя углубленное изучение юридических текстов, этических руководств и практических примеров, обеспечивая всестороннее понимание рассматриваемых вопросов. Юридический обзор фокусируется на анализе соответствующих законов, положений и судебных толкований для выявления правовых последствий хранения данных в блокчейне.

Качественный анализ выбран из-за его способности предоставлять богатые, подробные сведения о сложном взаимодействии между технологией, правом и этикой. Этот подход позволяет провести исследовательское исследование того, как технология блокчейн пересекается с устоявшимися правовыми и этическими рамками. Кроме того, систематический юридический обзор необходим для понимания конкретных правовых требований и ограничений, которые применяются к реализациям блокчейна.

2.2. Сбор данных. Сбор данных для этого исследования включает сбор информации из трех основных источников: юридических документов, этических рекомендаций и примеров внедрения блокчейна.

Юридические документы: исследование рассматривает ключевые правовые положения и положения, касающиеся защиты персональных данных и технологии блокчейна. Сюда входят Общий регламент по защите данных (GDPR) Европейского союза, Закон Калифорнии о защите прав потребителей (CCPA) и другие соответствующие национальные и международные законы.

Исследования случаев: Практические исследования случаев внедрения блокчейна, включающие хранение персональных данных, изучаются для понимания того, как теоретические принципы применяются в реальных сценариях. Исследования случаев выбираются на основе их релевантности и значимости, охватывая широкий спектр приложений от здравоохранения до финансовых услуг.

2.3. Анализ. Аналитическая структура для этого исследования включает три ключевых компонента: юридический анализ, этический анализ и оценку тематического исследования.

Юридический анализ фокусируется на выявлении и интерпретации соответствующих юридических требований и ограничений для хранения персональных данных в блокчейне. Это включает изучение конкретных положений GDPR, CCPA и других соответствующих законов, а также понимание их последствий для технологии блокчейн. Экспертные мнения ученых-юристов и практиков включены для обеспечения детального понимания этих юридических текстов. Например, Фойгт и фон дем Буше предоставляют практическое руководство по GDPR, подчеркивая проблемы и потенциальные решения для соответствия блокчейну.

III. Полученные результаты

3.1. Правовой анализ

Обзор соответствующих законов и нормативных актов

Правовой ландшафт хранения персональных данных в блокчейне формируется всеобъемлющими законами о защите данных, такими как Общий регламент по защите данных (GDPR) в Европейском союзе и Закон Калифорнии о защите прав потребителей (CCPA) в Соединенных Штатах. GDPR, вступивший в силу с мая 2018 года, устанавливает строгие требования к защите данных и конфиденциальности, подчеркивая права людей на их персональные данные. Аналогичным образом, CCPA, вступивший в силу в январе 2020 года, усиливает права на конфиденциальность и защиту потребителей для жителей Калифорнии, США.

3.2. Этические соображения

Такие этические принципы, как конфиденциальность, согласие и прозрачность, имеют первостепенное значение в контексте хранения персональных данных. Конфиденциальность гарантирует, что люди имеют контроль над своей личной информацией и тем, как она передается. Согласие требует, чтобы люди были полностью информированы и соглашались с тем, как используются их данные. Прозрачность подразумевает открытость в отношении методов работы с данными и четкое общение с субъектами данных.

Технология блокчейна представляет определенные этические дилеммы.

Неизменность блокчейна, хотя и обеспечивает целостность данных, противоречит этическому принципу права на забвение. По словам Зискинда, Натана и Пентланда, неизменная природа блокчейна может потенциально нарушать права людей на изменение или удаление своей личной информации, что вызывает серьезные этические проблемы.

Право собственности на данные является еще одним критически важным этическим вопросом. В децентрализованном блокчейне право собственности на данные часто неоднозначно. Такое отсутствие четкого права собственности может привести к этическим проблемам, особенно когда речь идет о персональных данных. Как подчеркивает Фэрфилд, децентрализованная природа блокчейна усложняет установление четкого права собственности на данные, что может привести к спорам и этическим конфликтам. Кроме того, получение подлинного согласия является сложной задачей в приложениях блокчейна. Пользователи могут не полностью понимать долгосрочные последствия хранения своих данных в неизменяемом реестре. Купс и Линес утверждают, что осознанное согласие в контексте блокчейна трудно достичь, поскольку пользователи могут не понимать всей степени постоянства данных и его будущих последствий.

4. Обсуждение. Правовой анализ показывает, что текущие правила защиты данных, такие как GDPR и CCPA, создают значительные проблемы для использования технологии блокчейна для хранения персональных данных. Право GDPR на удаление или «право быть забытым» напрямую противоречит неизменяемой природе блокчейна, представляя собой существенное юридическое препятствие. Этот вывод подчеркивает необходимость для разработчиков блокчейна разрабатывать новые решения, которые могут примирить эти различия, такие как хранение вне цепочки или гибридные модели, в которых конфиденциальные данные хранятся вне цепочки, а в цепочке хранятся только важные точки данных или ссылки.

CCPA также подчеркивает контроль потребителей над персональными данными, включая право отказаться от продажи данных и требование к компаниям раскрывать категории собранной личной информации. Поэтому реализации блокчейна должны включать механизмы для обеспечения соответствия, такие как разрешение потребителям контролировать свои данные с помощью шифрования и предоставление прозрачного раскрытия информации об использовании данных.

Этические дилеммы и потенциальные решения

Этический анализ подчеркивает критические дилеммы, включая конфликт между правами на неприкосновенность частной жизни и прозрачностью и неизменностью блокчейна. Этический принцип конфиденциальности требует, чтобы люди имели контроль над своей личной информацией, что может подорвать неизменяемая природа блокчейна. Чтобы решить эту проблему, разработчики могут принять технологии, повышающие конфиденциальность, такие как доказательства с нулевым разглашением, которые позволяют проверять данные, не раскрывая сами данные. Согласие — еще одна важная этическая проблема. Осознанное согласие требует, чтобы люди полностью понимали, как будут использоваться их данные, что может быть сложно из-за сложной и технической природы блокчейна. Улучшение пользовательских интерфейсов для предоставления четкой и краткой информации об использовании данных, а также использование инициатив по обучению пользователей могут помочь обеспечить осознанное согласие.

Заключение. Пересечение технологии блокчейна с правовыми и этическими соображениями хранения персональных данных представляет собой сложный, но проходимый ландшафт. Результаты этого исследования подчеркивают существенные проблемы, связанные с законами о защите данных и этическими принципами, но также предлагают потенциальные решения и стратегии для соблюдения и этической практики. Принимая гибридные модели хранения, технологии повышения конфиденциальности и механизмы согласия, ориентированные на пользователя, разработчики и организации блокчейна могут лучше согласовывать свою практику с правовыми и этическими требованиями. Кроме того, постоянное сотрудничество между

регулирующими органами и технологами, наряду с постоянными аудитами и проверками соответствия, будет иметь решающее значение для обеспечения того, чтобы реализации блокчейна были как юридически обоснованными, так и этически ответственными. Рекомендации, представленные в этом исследовании, направлены на содействие сбалансированному подходу, который использует преимущества блокчейна, одновременно защищая персональные данные и отстаивая индивидуальные права.

Библиография

1. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. 2016 2nd International Conference on Open and Big Data (OBD), 25-30. https://doi.org/10.1109/OBD.2016.11
2. Buterin, V. (2016). On Public and Private Blockchains. Retrieved from https://ethereum.github.io/blog/2016/08/07/on-public-and-private-blockchains/
3. Fairfield, J. (2014). BitProperty. Southern California Law Review, 88(805). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505915
4. Finck, M. (2018). Blockchains and Data Protection in the European Union. European Data Protection Law Review, 4(1), 17-35. https://doi.org/10.21552/edpl/2018/1/6
5. Floridi, L. (2013). The Ethics of Information. Oxford University Press.
6. Graglia, J. M., & Mellon, C. (2018). Blockchain and Property in 2018: At the End of the Beginning. Innovations: Technology, Governance, Globalization, 12(1-2), 90-116. https://doi.org/10.1162/inov_a_00271
7. Koops, B. J., & Leenes, R. (2014). Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provisions in Data-Protection Law. International Review of Law, Computers & Technology, 28(2), 159-171. https://doi.org/10.1080/13600869.2013.801589
8. Kuner, C. (2020). The CCPA and GDPR: Understanding the Key Differences. Privacy Laws & Business International Report, 2020(162), 1-4. Retrieved from https://www.privacylaws.com/reports/int162.pdf
9. Mettler, M. (2016). Blockchain Technology in Healthcare: The Revolution Starts Here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 1-3. https://doi.org/10.1109/HealthCom.2016.7749510
10. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187. https://doi.org/10.1007/s12599-017-0467-3
11. Rostamy, R., & Nilsson, E. (2020). Blockchain Technology and GDPR Compliance: Can They Be Reconciled? European Journal of Law and Technology, 11(1). Retrieved from https://ejlt.org/index.php/ejlt/article/view/730
12. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.
13. Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7
14. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops, 180-184. https://doi.org/10.1109/SPW.2015.27