ISSN: 2053-3578 I.F. 9.1

БЛОКЧЕЙН И КОНФИДЕНЦИАЛЬНОСТЬ: БАЛАНС МЕЖДУ ПРОЗРАЧНОСТЬЮ И ЗАЩИТОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

Ключевые слова: *Технология блокчейн, Персональные данные, GDPR, Конфиденциальность данных, Соблюдение законодательства, Неизменяемость, Защита данных, право на забвение, криптографические методы, соответствие*

Аннотация

В этой статье рассматривается пересечение технологии блокчейна и права на конфиденциальность, с упором на проблемы, связанные с GDPR. Основные характеристики блокчейна, такие как децентрализация и неизменность, часто противоречат правилам конфиденциальности, в частности праву на забвение. В исследовании рассматриваются технические решения, такие как гибридное управление данными и технологии повышения конфиденциальности, а также призываются к адаптивным правовым рамкам. Результаты подчеркивают необходимость междисциплинарного сотрудничества для использования преимуществ блокчейна при обеспечении соблюдения законов о конфиденциальности.

I. Введение

Технология блокчейна стала преобразующей силой в различных отраслях, кардинально изменив то, как данные хранятся, передаются и защищаются. По своей сути блокчейн — это децентрализованный распределенный реестр, который записывает транзакции на многих компьютерах таким образом, что зарегистрированные транзакции не могут быть изменены задним числом[1]. Эта неизменность, наряду с присущей блокчейну

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

прозрачностью, где каждая транзакция видна всем участникам сети, дает значительные преимущества с точки зрения безопасности, доверия и эффективности[2].

Внедрение технологии блокчейна особенно заметно в таких секторах, как финансы, здравоохранение, управление цепочками поставок и государственные услуги, где потребность в безопасном и прозрачном управлении данными имеет первостепенное значение[3]. Например, в финансах блокчейн является основой криптовалют, таких как биткоин и эфириум, обеспечивая безопасные одноранговые транзакции без необходимости в посредниках. В здравоохранении блокчейн изучается для безопасного управления данными пациентов, в то время как в цепочках поставок он используется для отслеживания товаров от источника до потребителя, обеспечивая подлинность и снижая мошенничество[4]. Однако те самые особенности, которые делают блокчейн таким мощным — децентрализация, неизменность и прозрачность — также представляют значительные проблемы, особенно в контексте права на конфиденциальность. Законы о конфиденциальности, такие как Общий регламент по защите данных (GDPR) в Европейском союзе, подчеркивают защиту персональных данных, предоставляя людям права на то, как их данные собираются, хранятся и удаляются[5]. Неизменная и прозрачная природа блокчейна может противоречить этим требованиям, особенно в отношении права на забвение и принципов минимизации данных[6]. Это внутреннее противоречие поднимает важные вопросы о том, как технология блокчейн может быть согласована с необходимостью защиты персональных данных, что требует более тщательного изучения как технологических, так и правовых рамок, чтобы гарантировать, что преимущества блокчейна не будут достигаться за счет конфиденциальности.

II. Методы

Обзор литературы

[2] Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104-113. https://doi.org/10.1145/2701411

[3] Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin.

[4] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068

[5] 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

[6] Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27

Основа этого исследования основана на обширном обзоре литературы, направленном на понимание пересечения между технологией блокчейна и законодательством о конфиденциальности. Обзор включал тщательное изучение рецензируемых статей, юридических документов, официальных документов и тематических исследований, опубликованных за последнее десятилетие. Для поиска соответствующих материалов использовались такие ключевые базы данных, как IEEE Xplore, SpringerLink, JSTOR и Google Scholar. Основное внимание уделялось выявлению как технических аспектов блокчейна (например, децентрализации, неизменности, прозрачности), так и правовых последствий, особенно в соответствии с правилами конфиденциальности, такими как Общий регламент по защите данных (GDPR)[7]. В обзор также были включены статьи, в которых обсуждаются технические решения, предлагаемые для решения проблем конфиденциальности в блокчейне, такие как доказательства с нулевым разглашением и хранение вне цепочки[8]. Этот комплексный подход обеспечил всестороннее понимание текущего ландшафта и проблем на стыке блокчейна и права конфиденциальности.

Анализ примеров

Чтобы предоставить практическое представление о том, как технология блокчейна взаимодействует с правом конфиденциальности, было проанализировано несколько исследований примеров из разных отраслей. Эти исследования примеров были выбраны на основе их релевантности для важных вопросов конфиденциальности и внедрения технологии блокчейна способами, которые подчеркивают напряженность между прозрачностью и защитой данных. Выбранные секторы включают финансы, здравоохранение и управление цепочками поставок, все из которых обрабатывают конфиденциальные персональные данные и, таким образом, подчиняются строгим правилам конфиденциальности.

В финансовом секторе исследование изучало использование блокчейна в криптовалютных транзакциях, уделяя особое внимание тому, как публичные и частные сети блокчейнов управляют идентификацией пользователей и данными транзакций, пытаясь при этом

[7] https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf
[8] Finck, M. (2018). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? European Law Journal, 24(1), 29-41. https://doi.org/10.1111/eulj.12272

соблюдать требования GDPR[9]. В здравоохранении в тематических исследованиях рассматривались системы управления данными пациентов на основе блокчейна, в частности, то, как эти системы решают вопросы согласия и права на забвение в соответствии с законами о конфиденциальности[10]. Для управления цепочками поставок анализ был сосредоточен на роли блокчейна в отслеживании товаров и проблемах поддержания прозрачности при защите персональных данных лиц, участвующих в цепочке поставок[11].

Правовой анализ

Правовой анализ был направлен на понимание последствий технологии блокчейна для существующих законов о конфиденциальности с акцентом на GDPR. Исследование систематически рассматривало ключевые статьи GDPR, такие как статья 17 (Право на удаление) и статья 25 (Защита данных по проекту и по умолчанию), в контексте системы неизменяемого реестра блокчейна[12]. Также был проведен сравнительный правовой анализ, чтобы изучить, как различные юрисдикции, включая Европейский союз и Соединенные Штаты, подходят к регулированию технологии блокчейна с точки зрения конфиденциальности. Это включало рассмотрение нормативных рекомендаций, юридических комментариев и политических документов.

Особое внимание было уделено юридическим комментариям, в которых обсуждается совместимость характеристик блокчейна с требованиями GDPR. Например, критически проанализирована концепция минимизации данных и то, как ее можно согласовать с тенденцией блокчейна хранить комплексные транзакционные данные в течение неопределенного срока[13]. В исследовании также изучались потенциальные правовые рамки, которые могли бы позволить блокчейну работать в рамках закона о конфиденциальности,

[9] Kugler, L. (2018). Why cryptocurrencies use so much energy. Communications of the ACM, 61(7), 15-17. https://doi.org/10.1145/3213763

[10] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068

[11] Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In 2016 13th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSSM.2016.7538424

[12] 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

[13] Finck, M. (2018). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? European Law Journal, 24(1), 29-41. https://doi.org/10.1111/eulj.12272

такие как гибридные модели, которые объединяют управление данными в цепочке и вне ее[14].

III. Результаты

Основные выводы из обзора литературы

Обзор литературы выявил существенные сведения о пересечении технологии блокчейна и права на конфиденциальность. Одним из основных выводов было то, что, хотя блокчейн обеспечивает повышенную безопасность и прозрачность, эти функции могут противоречить правилам конфиденциальности, особенно в контексте GDPR. Исследование Финка подчеркнуло, что неизменяемая природа блокчейна создает проблемы для соблюдения права на забвение, фундаментального аспекта GDPR, который позволяет людям запрашивать удаление своих персональных данных[15]. Это несоответствие было дополнительно подтверждено Зискиндом и Натаном[16], которые обсуждали, как присущая блокчейну прозрачность может подорвать конфиденциальность пользователя, раскрывая детали транзакций, что противоречит принципам минимизации данных и ограничения цели, изложенным в GDPR.

Другим важным выявленным аспектом были различные подходы к защите данных в разных юрисдикциях. В то время как в ЕС действуют строгие законы о конфиденциальности, в США применяется более фрагментарный подход, ориентированный на отраслевые правила, а не на комплексную защиту данных. Это несоответствие может создать проблемы для организаций, стремящихся внедрить решения на основе блокчейна, соответствующие нескольким правовым рамкам[17]. Кроме того, в литературе указано, что многие организации по-прежнему не понимают последствий блокчейна для конфиденциальности данных, что приводит к нерешительности в отношении полного внедрения технологии[18].

Выводы из тематических исследований

[14] Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27
[15] Finck, M. (2018). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? European Law Journal, 24(1), 29-41. https://doi.org/10.1111/eulj.12272
[16] Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27
[17] 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
[18] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068

Проанализированные тематические исследования предоставили практические примеры того, как блокчейн используется в различных отраслях, подчеркнув как проблемы, так и инновационные решения для решения проблем конфиденциальности. Например, в финансовом секторе использование публичных блокчейнов для криптовалютных транзакций вызвало серьезные проблемы конфиденциальности. Ярким примером является внедрение криптовалют, ориентированных на конфиденциальность, таких как Monero и Zcash, которые используют передовые криптографические методы для повышения конфиденциальности пользователей[19]. Эти криптовалюты демонстрируют, как блокчейн можно адаптировать для лучшего соответствия принципам конфиденциальности, позволяя пользователям участвовать в транзакциях, не раскрывая свои личности или детали транзакций.

В секторе здравоохранения исследование на основе блокчейн-систем управления данными пациентов проиллюстрировало потенциал для улучшения конфиденциальности пациентов при одновременном повышении безопасности данных. Такие платформы, как MedRec, используют блокчейн, чтобы позволить пациентам контролировать доступ к своим медицинским записям, обеспечивая более ориентированный на пациента подход к управлению данными[20]. Это исследование показало, что блокчейн может способствовать соблюдению требований GDPR о согласии, предоставляя пациентам прозрачный контроль над тем, кто получает доступ к их данным. Однако в исследовании также отмечены проблемы, такие как необходимость взаимодействия между блокчейн-системами и существующей инфраструктурой здравоохранения, что может усложнить реализацию решений по сохранению конфиденциальности.

Анализ управления цепочкой поставок выявил потенциал блокчейна для повышения прозрачности при одновременном повышении проблем с конфиденциальностью. Например, такие компании, как IBM и Walmart, внедрили решения на основе блокчейна для улучшения прослеживаемости в цепочках поставок продуктов питания, гарантируя безопасность и подлинность продуктов[21]. Хотя эти системы способствуют прозрачности,

[19] Kugler, L. (2018). Why cryptocurrencies use so much energy. Communications of the ACM, 61(7), 15-17. https://doi.org/10.1145/3213763

[20] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068

[21] Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In 2016 13th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSSM.2016.7538424

они также рискуют раскрыть конфиденциальные данные о поставщиках и производственных процессах. В исследовании подчеркивалась необходимость тщательного рассмотрения того, какие данные хранятся в цепочке, и возможности решений для хранения вне цепочки для снижения рисков конфиденциальности.

Результаты юридического анализа

Юридический анализ выявил критические пробелы между технологией блокчейна и существующими законами о конфиденциальности. Изучение статей GDPR выявило проблемы, которые блокчейн создает для права на удаление, поскольку после записи данных в блокчейн их нельзя легко изменить или удалить[22]. Эта несовместимость поднимает вопросы о том, как организации могут согласовать неизменную природу блокчейна с юридическими обязательствами по выполнению запросов субъектов данных на удаление данных.

В анализе также изучались потенциальные правовые рамки, которые могли бы облегчить интеграцию блокчейна в существующие правила конфиденциальности. Одним из перспективных подходов, обсуждавшихся в ходе обсуждения, была реализация гибридных моделей, которые объединяют управление данными в цепочке и вне ее. Храня персональные данные вне цепочки и используя блокчейн для проверки и аудита, организации могут поддерживать соблюдение законов о конфиденциальности, используя преимущества технологии блокчейна[23]. Кроме того, исследование доказательств с нулевым разглашением и других криптографических методов представило жизнеспособные варианты для повышения конфиденциальности в публичных блокчейнах, позволяя проводить проверку без раскрытия персональных данных[24].

IV. Обсуждение

Результаты этого исследования подчеркивают тонкие и сложные отношения между технологией блокчейна и законодательством о конфиденциальности, особенно в рамках GDPR. Анализ показывает, что хотя основные характеристики блокчейна — децентрализация, неизменность и прозрачность — предлагают значительные

[22] 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
[23] Finck, M. (2018). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? European Law Journal, 24(1), 29-41. https://doi.org/10.1111/eulj.12272
[24] Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27

преимущества с точки зрения безопасности и доверия, они также создают проблемы в выполнении требований конфиденциальности.

Одной из основных выявленных проблем является конфликт между неизменностью блокчейна и правом GDPR на забвение. Невозможность удалить данные после того, как они были записаны в блокчейн, представляет собой значительную проблему для организаций, стремящихся выполнить запросы на удаление данных[25]. Этот конфликт подчеркивает необходимость инновационных технических решений и адаптивных правовых рамок. Например, исследование предполагает, что гибридные модели, которые объединяют управление данными в цепочке и вне ее, могут предложить жизнеспособное решение, позволяя хранить конфиденциальные данные вне цепочки при использовании блокчейна для целей проверки[26].

Кроме того, анализы случаев в исследовании в различных отраслях показывают, что, хотя блокчейн может повысить прозрачность и прослеживаемость, он также может раскрыть конфиденциальные персональные данные, потенциально нарушая принципы минимизации данных и ограничения цели в соответствии с GDPR [27]. Этот вывод особенно актуален для таких отраслей, как финансы и здравоохранение, где защита персональных данных имеет первостепенное значение. Использование технологий, повышающих конфиденциальность, таких как доказательства с нулевым разглашением и передовые криптографические методы, по-видимому, является многообещающим подходом к решению этих проблем[28]. Однако широкое внедрение этих технологий остается ограниченным из-за технической сложности и соображений стоимости.

Экспертные интервью дополнительно подчеркивают необходимость большей осведомленности и просвещения относительно последствий технологии блокчейн для конфиденциальности. Меняющийся нормативный ландшафт также требует тесного сотрудничества между технологами, юристами и политиками, чтобы гарантировать, что

[25] Finck, M. (2018). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? European Law Journal, 24(1), 29-41. https://doi.org/10.1111/eulj.12272
[26] Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27
[27] Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In 2016 13th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSSM.2016.7538424
[28] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068

проблемы конфиденциальности будут решаться без подавления инноваций. Интервью предполагают, что будущие усилия по регулированию должны быть сосредоточены на создании адаптивных структур, которые могут учитывать уникальные характеристики блокчейна, защищая при этом права на частную жизнь отдельных лиц[29].

В заключение следует отметить, что, хотя технология блокчейна предлагает преобразующий потенциал в различных отраслях, она также создает значительные проблемы для соблюдения законов о конфиденциальности. Решение этих проблем требует многогранного подхода, включающего технологические инновации, правовую адаптацию и междисциплинарное сотрудничество. Проактивно решая проблемы конфиденциальности, можно использовать преимущества технологии блокчейна, обеспечивая при этом соблюдение прав отдельных лиц.

V. Заключение

В этом исследовании изучалась сложная связь между технологией блокчейна и законодательством о конфиденциальности, особенно в контексте GDPR. Хотя блокчейн предлагает существенные преимущества с точки зрения безопасности, прозрачности и децентрализации, эти же особенности создают значительные проблемы для соблюдения конфиденциальности. Неизменная природа блокчейна противоречит праву GDPR на забвение, а прозрачный характер транзакций может раскрыть персональные данные, нарушая такие принципы, как минимизация данных.

Для решения этих проблем исследование предлагает сочетание технических инноваций, таких как доказательства с нулевым разглашением и гибридные модели управления данными, а также правовые адаптации, которые лучше согласуют блокчейн с существующими структурами конфиденциальности. Результаты также подчеркивают необходимость постоянного сотрудничества между технологами, юристами и политиками для разработки адаптивных правил, которые защищают конфиденциальность, не препятствуя инновациям.

Подводя итог, можно сказать, что, хотя блокчейн имеет большие перспективы, его успешная интеграция в отрасли, подпадающие под действие законов о конфиденциальности, требует тщательного рассмотрения как технологических, так и юридических факторов. Проактивно решая эти проблемы, можно использовать

[29] 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

преимущества блокчейна, обеспечивая при этом соблюдение правил конфиденциальности, тем самым укрепляя доверие и способствуя более широкому внедрению этой преобразующей технологии.

Список использованной литературы

1. Finck, M. (2018). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? European Law Journal, 24(1), 29-41. https://doi.org/10.1111/eulj.12272
2. Kugler, L. (2018). Why cryptocurrencies use so much energy. Communications of the ACM, 61(7), 15-17. https://doi.org/10.1145/3213763
3. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068
4. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf
5. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin.
6. Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In 2016 13th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSSM.2016.7538424
7. 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
8. Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104-113. https://doi.org/10.1145/2701411
9. Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27
10. https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf