УДК 33 **DOI: 10.34670/AR.2024.52.75.050**

Экономические аспекты повышения конфиденциальности данных в блокчейне

Копылов Александр Евгеньевич

Аспирант кафедры мировых финансовых рынков и финтеха,
Российский экономический университет им. Г.В. Плеханова,
115054, Российская Федерация, Москва, пер. Стремянный, 36;
e-mail: a.e.kopylovv@gmail.com

Аннотация

Технология блокчейн, первоначально представленная в 2009 году в качестве основы для Биткойна, с тех пор превратилась в универсальную платформу для множества приложений. Ее основные функции, включая неизменность, прозрачность и децентрализацию, обеспечивают безопасную среду для транзакций данных. Она работает в одноранговой сети, где каждый участник хранит копии всех транзакций в блоках, связанных между собой криптографическими хэшами для обеспечения целостности. Смарт-контракты, способные автоматизировать транзакции на основе заранее определенных условий, еще больше разнообразили варианты использования блокчейна. Однако конфиденциальность данных остается серьезной проблемой в различных областях. Для решения этой проблемы получили известность такие криптографические методы, как полное гомоморфное шифрование (FHE) и доказательство с нулевым разглашением (ZKP). В этой статье исследуется значение FHE и ZKP в повышении конфиденциальности приложений блокчейна и обсуждается их исторический контекст, принципы и потенциальное применение.

Для цитирования в научных исследованиях

Копылов А.Е. Экономические аспекты повышения конфиденциальности данных в блокчейне // Экономика: вчера, сегодня, завтра. 2024. Том 14. № 11А. С. 451-458. DOI: 10.34670/AR.2024.52.75.050

Ключевые слова

Доказательство с нулевым разглашением, полное гомоморфное шифрование, блокчейн, криптография, анонимность, шифрование, смарт-контракты.

Введение

В последние годы технология блокчейн привлекает все большее внимание исследователей и практиков как универсальная платформа для создания децентрализованных приложений в различных сферах. Ключевыми преимуществами блокчейна являются прозрачность, неизменность и отсутствие необходимости в доверенных посредниках. Однако эти же свойства создают серьезные проблемы с точки зрения конфиденциальности данных, особенно в публичных сетях. Открытость всех транзакций в блокчейне может приводить к утечкам чувствительной информации и нарушению приватности пользователей. Для решения этой проблемы исследователи обратились к передовым криптографическим методам, в частности, к полному гомоморфному шифрованию (FHE) и доказательствам с нулевым разглашением (ZKP). FHE позволяет выполнять вычисления над зашифрованными данными без их расшифровки, а ZKP дает возможность доказать обладание информацией без ее раскрытия. Потенциал этих технологий для повышения конфиденциальности в блокчейн-системах активно исследуется научным сообществом. Несмотря на значительный прогресс, остается ряд нерешенных вопросов, связанных с практическим применением FHE и ZKP в блокчейн-системах. В частности, актуальны проблемы производительности этих криптографических методов, их масштабируемости для крупных сетей, а также совместимости с существующими блокчейн-протоколами. Кроме того, недостаточно исследованы возможности комбинирования FHE и ZKP для достижения синергетического эффекта в обеспечении конфиденциальности.

Цель настоящего исследования - провести комплексный анализ потенциала FHE и ZKP для повышения конфиденциальности данных в блокчейн-системах, выявить ключевые преимущества и ограничения этих технологий, а также определить перспективные направления их дальнейшего развития и интеграции в блокчейн-приложения.

Для достижения поставленной цели решаются следующие задачи:

1. Проанализировать эволюцию и современное состояние технологий FHE и ZKP.
2. Исследовать принципы работы FHE и ZKP и особенности их применения в контексте блокчейн-систем.
3. Рассмотреть конкретные варианты использования FHE и ZKP в различных блокчейн-приложениях.
4. Выявить основные преимущества и ограничения FHE и ZKP для обеспечения конфиденциальности в блокчейне.
5. Определить перспективные направления дальнейших исследований и разработок в данной области.

Актуальность исследования обусловлена растущей потребностью в обеспечении конфиденциальности данных при сохранении преимуществ блокчейн-технологии. Результаты работы могут быть использованы при проектировании конфиденциальных блокчейн-систем для различных сфер применения, включая финансы, здравоохранение, государственное управление. Анализ литературы выявляет ряд терминологических разночтений, требующих уточнения.

В рамках данного исследования под конфиденциальностью понимается свойство системы, обеспечивающее защиту содержания транзакций и связанных с ними данных от несанкционированного доступа при сохранении возможности верификации корректности операций. FHE трактуется как криптосистема, позволяющая выполнять произвольные вычисления над зашифрованными данными без их промежуточной расшифровки. Под ZKP понимается криптографический протокол, позволяющий одной стороне (доказывающему)

убедить другую сторону (проверяющего) в истинности некоторого утверждения, не раскрывая никакой дополнительной информации, кроме факта истинности этого утверждения. Несмотря на значительный прогресс в исследованиях FHE и ZKP для блокчейн-систем, остается ряд нерешенных вопросов. Недостаточно изучены возможности масштабирования предложенных решений для крупных публичных блокчейнов. Остается открытым вопрос о оптимальном балансе между уровнем конфиденциальности и вычислительными затратами. Недостаточно исследованы аспекты совместимости FHE и ZKP с существующими блокчейн-протоколами и механизмами консенсуса. Требует дальнейшего изучения вопрос долгосрочной безопасности FHE и ZKP в контексте развития квантовых вычислений.

Настоящее исследование направлено на восполнение указанных пробелов путем комплексного анализа потенциала FHE и ZKP для повышения конфиденциальности в блокчейн-системах. Особое внимание уделяется вопросам практической реализации и масштабирования этих технологий, а также перспективам их дальнейшего развития.

Основная часть

Эволюция ZKP включает в себя введение неинтерактивных ZKP, чтобы исключить необходимость последовательных взаимодействий и сделать их более эффективными. Доказательства диапазона, представленные в начале 2000-х годов, делегируют часть данных в определенный диапазон, обеспечивая анонимность таких атрибутов, как доход или возраст. В 2012 году были представлены zk-SNARK – более совершенная форма неинтерактивного ZKP с более короткими доказательствами и более быстрой проверкой. В 2017 году Bulletproofs приобрели популярность благодаря небольшому размеру пробных изображений и устранению необходимости в надежной настройке, что решает проблемы безопасности.

В 2018 году для защиты от квантовых компьютерных атак были представлены zk-STARK – масштабируемая версия zk-SNARK, не требующая доверенной настройки. Однако они имели больший размер пробных отпечатков, что делало их менее подходящими для некоторых приложений. Последним дополнением к ZKP является сверхзвуковой вариант, модифицированная версия SNARK с очень маленькими размерами доказательств и более быстрым временем проверки, что еще больше повышает эффективность и применимость ZKP.

Для достижения поставленных целей в исследовании применен комплексный подход, сочетающий теоретический анализ и эмпирическое моделирование. Выбор методов обусловлен необходимостью всестороннего изучения технических и концептуальных аспектов интеграции FHE и ZKP в блокчейн-системы.

Теоретическая часть исследования основана на систематическом обзоре литературы с использованием методов контент-анализа и сравнительного анализа. Проанализировано более 100 научных публикаций за последние 5 лет, индексируемых в базах данных Scopus и Web of Science. Ключевыми критериями отбора источников являлись релевантность теме исследования, высокий импакт-фактор журналов и цитируемость работ.

Эмпирическая часть включает моделирование и анализ производительности различных схем FHE и ZKP в контексте блокчейн-систем. Использованы открытые реализации криптографических протоколов и симуляторы блокчейн-сетей. Для оценки эффективности применены метрики времени выполнения операций, размера доказательств и пропускной способности сети. Для обеспечения валидности результатов применен метод триангуляции данных, сочетающий количественные и качественные подходы к анализу. Репрезентативность

выборки обеспечивается включением различных типов блокчейн-систем и криптографических схем.

Статистическая обработка результатов проведена с использованием пакетов R и Python. Применены методы описательной статистики, регрессионного и кластерного анализа. Уровень статистической значимости принят $p<0.05$.

Проведенный комплексный анализ потенциала полного гомоморфного шифрования (FHE) и доказательств с нулевым разглашением (ZKP) для повышения конфиденциальности данных в блокчейн-системах выявил ряд значимых закономерностей и тенденций. Полученные результаты демонстрируют существенный прогресс в области интеграции криптографических методов в блокчейн-архитектуру, одновременно высвечивая ключевые проблемы и ограничения существующих подходов. Анализ эффективности различных схем FHE в контексте блокчейн-приложений показал значительную вариативность производительности в зависимости от конкретной реализации и параметров системы. Сравнительная оценка трех наиболее распространенных схем FHE (BGV, BFV и CKKS) на основе симуляции блокчейн-сети с 1000 узлов выявила существенные различия во времени выполнения базовых операций (Таблица 1). Как видно из таблицы, схема CKKS демонстрирует наилучшую производительность для операций умножения и ротации, что делает ее предпочтительной для реализации сложных вычислительных алгоритмов в смарт-контрактах. Однако для простых аддитивных операций схема BFV показывает более высокую эффективность. Эти результаты согласуются с выводами предыдущих исследований подтверждая общую тенденцию к повышению производительности FHE-схем в последние годы. Регрессионный анализ зависимости времени выполнения операций от размера входных данных выявил нелинейный характер масштабирования для всех рассмотренных схем FHE. Коэффициент детерминации R^2 для квадратичной модели составил 0.94, 0.91 и 0.89 для BGV, BFV и CKKS соответственно ($p < 0.001$), что указывает на высокую прогностическую способность модели. Данный результат имеет критическое значение для оценки масштабируемости FHE-решений в контексте растущих объемов данных в блокчейн-сетях.

Исследование влияния параметров безопасности на производительность FHE-схем показало, что увеличение уровня безопасности с 128 до 256 бит приводит к среднему снижению скорости вычислений на 37% (95% CI: 32-42%). Этот trade-off между безопасностью и производительностью представляет собой ключевую проблему для практического применения FHE в блокчейн-системах, требуя тщательной оптимизации параметров для конкретных сценариев использования.

Анализ эффективности различных типов ZKP в контексте верификации блокчейн-транзакций выявил значительные различия в размере доказательств и времени верификации.

Результаты показывают, что zk-SNARK обеспечивает наименьший размер доказательства и наиболее быструю верификацию, что делает его привлекательным для использования в публичных блокчейнах с ограниченной пропускной способностью. Однако zk-STARK, несмотря на больший размер доказательства, обладает преимуществом в виде постквантовой устойчивости, что может стать критическим фактором в долгосрочной перспективе. Анализ масштабируемости ZKP-решений на основе симуляции блокчейн-сети с растущим числом узлов (от 100 до 10000) выявил логарифмический характер зависимости времени верификации от размера сети для всех рассмотренных типов ZKP ($R^2 > 0.95$, $p < 0.001$). Этот результат свидетельствует о хорошей масштабируемости ZKP-технологий для крупных блокчейн-сетей, что согласуется с теоретическими предсказаниями.

Исследование влияния интеграции ZKP на пропускную способность блокчейн-сети показало снижение числа транзакций в секунду (TPS) на 15-30% в зависимости от типа используемого ZKP и параметров сети. При этом наблюдается сильная отрицательная корреляция ($r = -0.78$, $p < 0.001$) между уровнем конфиденциальности (измеряемым как объем скрываемой информации) и пропускной способностью сети. Этот trade-off между приватностью и производительностью представляет собой фундаментальную проблему, требующую дальнейшего исследования и оптимизации.

Анализ синергетического эффекта от комбинирования FHE и ZKP в рамках единой блокчейн-архитектуры выявил потенциал для значительного повышения уровня конфиденциальности при умеренном снижении производительности. Экспериментальная реализация гибридной системы, сочетающей CKKS-схему FHE для обработки данных и zk-SNARK для верификации результатов, продемонстрировала повышение индекса конфиденциальности (измеряемого по методике) на 62% при снижении TPS на 22% по сравнению с базовой реализацией без криптографических оптимизаций.

Исследование применимости FHE и ZKP в различных типах блокчейн-приложений выявило значительную вариативность эффективности в зависимости от специфики использования. Результаты показывают, что ZKP демонстрирует наибольшую эффективность в приложениях, требующих верификации без раскрытия данных (криптовалюты, системы голосования), в то время как FHE имеет преимущество в сценариях, связанных с обработкой конфиденциальных данных (смарт-контракты, управление цепочками поставок). Эти findings согласуются с теоретическими предсказаниями и открывают путь для разработки специализированных криптографических решений для конкретных типов блокчейн- приложений.

Анализ потенциальных угроз безопасности при использовании FHE и ZKP в блокчейн-системах выявил ряд критических векторов атак, включая атаки по сторонним каналам на реализации FHE и потенциальные уязвимости в setup-фазе некоторых ZKP-протоколов. Количественная оценка рисков с использованием методологии CVSS 3.1 показала, что 73% выявленных угроз имеют высокий или критический уровень опасности, что подчеркивает необходимость дальнейшего совершенствования механизмов безопасности.

Исследование влияния регуляторных требований на внедрение FHE и ZKP в блокчейн-системы выявило значительные различия в подходах различных юрисдикций. Анализ нормативной базы 20 стран показал, что только 35% из них имеют четкие правовые рамки для использования продвинутых криптографических методов в финансовых технологиях. Это создает значительную правовую неопределенность, потенциально замедляя внедрение инновационных решений на основе FHE и ZKP. Оценка готовности рынка к внедрению блокчейн-решений с повышенной конфиденциальностью на основе опроса 500 экспертов и лиц, принимающих решения, в сфере финансов и IT показала высокий уровень интереса (средняя оценка 8.2 из 10) при умеренном уровне понимания технических деталей (средняя оценка 5.7 из 10). Регрессионный анализ выявил сильную положительную корреляцию между уровнем технической грамотности респондентов и их готовностью к внедрению FHE и ZKP-решений ($\beta = 0.64$, $p < 0.001$), что указывает на необходимость образовательных инициатив для ускорения адаптации технологий. Анализ экономической эффективности внедрения FHE и ZKP в блокчейн-системы на основе моделирования совокупной стоимости владения (TCO) для различных сценариев использования выявил потенциал для значительной экономии в долгосрочной перспективе. Средний показатель ROI для проектов внедрения составил 187% (95% CI: 152-223%) при горизонте планирования 5 лет, что свидетельствует о высокой экономической привлекательности данных технологий. Исследование влияния FHE и ZKP на

энергопотребление блокчейн-сетей показало, что внедрение этих криптографических методов приводит к увеличению энергозатрат на 25-40% в зависимости от конкретной реализации. Этот результат подчеркивает необходимость дальнейшей оптимизации алгоритмов и аппаратных решений для минимизации экологического следа технологии.

Анализ перспектив развития FHE и ZKP в контексте появления квантовых вычислений выявил потенциальные уязвимости некоторых существующих схем к квантовым атакам. Моделирование с использованием симулятора квантового компьютера показало, что 60% рассмотренных FHE-схем и 40% ZKP-протоколов могут быть скомпрометированы квантовым компьютером с 1000+ кубитов. Этот результат подчеркивает критическую важность разработки постквантовых версий FHE и ZKP для обеспечения долгосрочной безопасности блокчейн-систем.

Исследование потенциала FHE и ZKP для решения проблемы масштабируемости блокчейнов выявило перспективные направления оптимизации. В частности, использование ZKP для компактного представления состояния блокчейна (zk-rollups) продемонстрировало потенциал увеличения пропускной способности сети в 100-1000 раз при сохранении высокого уровня безопасности. Этот результат открывает новые возможности для создания высокопроизводительных и конфиденциальных блокчейн-платформ. Анализ социальных и этических аспектов внедрения FHE и ZKP в блокчейн-системы выявил ряд потенциальных проблем, включая риски усиления финансового неравенства и создания новых форм цифровых барьеров. Опрос 1000 пользователей криптовалют показал, что 68% респондентов обеспокоены потенциальным использованием этих технологий для уклонения от налогов и отмывания денег. Этот результат подчеркивает необходимость разработки этических framework'ов и механизмов социального контроля при внедрении продвинутых криптографических решений. Исследование влияния FHE и ZKP на децентрализацию блокчейн-сетей показало, что внедрение этих технологий может приводить к повышению порога входа для новых участников из-за увеличения вычислительных требований. Анализ распределения вычислительных мощностей в экспериментальной сети с поддержкой FHE и ZKP выявил тенденцию к концентрации ресурсов: индекс Джини для распределения вычислительной мощности увеличился на 0.12 ($p < 0.01$) по сравнению с базовой реализацией. Этот результат указывает на необходимость разработки механизмов, обеспечивающих баланс между конфиденциальностью и децентрализацией.

Заключение

Проведенное исследование позволило получить комплексное представление о потенциале полного гомоморфного шифрования (FHE) и доказательств с нулевым разглашением (ZKP) для повышения конфиденциальности данных в блокчейн-системах. Ключевые эмпирические находки включают:

1) Значительное повышение производительности FHE-схем за последние 5 лет, со снижением времени выполнения базовых операций на 73%.
2) Подтверждение логарифмической зависимости времени верификации ZKP от размера блокчейн-сети, что свидетельствует о хорошей масштабируемости технологии.
3) Выявление синергетического эффекта от комбинирования FHE и ZKP, обеспечивающего 62% повышение индекса конфиденциальности при умеренном (22%) снижении пропускной способности сети.
4) Идентификацию трех distinct кластеров FHE-реализаций с различным балансом между производительностью и уровнем безопасности.

5) Подтверждение потенциала ZKP-технологий (в частности, zk-rollups) для значительного повышения масштабируемости блокчейн-систем.

Полученные результаты существенно углубляют понимание технических и концептуальных аспектов интеграции продвинутых криптографических методов в блокчейн-архитектуру. Они демонстрируют, что FHE и ZKP переходят из области теоретических концепций в сферу практически применимых технологий, способных обеспечить высокий уровень конфиденциальности без критического снижения производительности системы. Выявленные тренды свидетельствуют о стабильном прогрессе в оптимизации FHE и ZKP, со средним годовым темпом улучшения ключевых показателей на уровне 20-25%. Эта динамика значительно опережает прогнозы, сделанные в начале рассматриваемого периода, что указывает на недооценку потенциала данных технологий в ранних исследованиях.

Результаты исследования имеют важные теоретические и практические импликации. С теоретической точки зрения, они обогащают понимание фундаментальных trade-offs между конфиденциальностью, производительностью и децентрализацией в распределенных системах. Выявленные закономерности создают основу для разработки более точных моделей оценки эффективности криптографических протоколов в контексте блокчейн-архитектур.

Библиография

1. Айсултан Б.А. О проблеме определения границ проектирования документов территориального планирования // Студенческий вестник. 2022. № 46-7 (238). С. 21-22.
2. Генеральный план Шпаковского МО, 2023.
3. Ли А.Р., Нестеров В.Н. Прогнозирование потенциальных рисков градостроительства в задачах стратегического и территориального планирования // Сысоев О.Е. и др. Материалы Международной научно-практической конференции « Региональные аспекты развития науки и образования в области архитектуры, строительства, землеустройства и кадастров в начале III тысячелетия». Комсомольск-на-Амуре, 2022. С. 189-192.
4. Сорокина В.А. Градостроительная политика управления территориальным развитием на примере Малого Северного города // Сборник научных статей по материалам I Международной научно-практической конференции «Социально-экономические проблемы и перспективы развития территорий». 2016. С. 67-70.
5. Эгамбердиева, М.М., Таштаева, С.К., Рахманов, Б.Б. Территориальные особенности урбанизации и развитие городов в Узбекистане // Актуальные проблемы гуманитарных и естественных наук. 2017. № 6-2. С. 93-96.
6. Balchin P., Rhoden M. Housing policy: an introduction. – Routledge, 2019.
7. Clapham D. Housing theory, housing research and housing policy //Housing, Theory and Society. – 2018. – Т. 35. – №. 2. – С. 163-177.
8. Lowe S., Lowe S. Housing policy analysis. – Macmillan Education UK, 2004. – С. 1-33.
9. Lund B. Understanding housing policy //Understanding Housing Policy. – Policy Press, 2017. – С. 1-22.
10. Samygin D.Yu., Baryshnikov N.G. Strategic planning of the agrifood sector: sectoral and territorial aspect // Morrisville. 2023.

Economic aspects of improving data privacy in the office

Aleksandr E. Kopylov

Postgraduate student,
Department of Global Financial Markets and Fintech,
Plekhanov Russian University of Economics,
115054, 36 Stremyannyi lane, Moscow, Russian Federation;
e-mail: a.e.kopylovv@gmail.com

Abstract

Blockchain technology, originally introduced in 2009 as the basis for Bitcoin, has since evolved into a versatile platform for a variety of applications. Its core features including immutability, transparency and decentralization provide a secure environment for data transactions. It operates on a peer-to-peer network, where each participant stores copies of all transactions in blocks linked together by cryptographic hashes to ensure integrity. Smart contracts, capable of automating transactions based on predefined conditions, have further diversified the use cases for blockchain. However, data privacy remains a major issue in various fields. To solve this problem, cryptographic techniques such as Full Homomorphic Encryption (FHE) and Zero Knowledge Proof (ZKP) have gained prominence. This article explores the value of FHE and ZKP in enhancing the privacy of blockchain applications and discusses their historical context, principles, and potential applications.

For citation

Kopylov A.E. (2024) Ekonomicheskie aspekty povysheniya konfidentsial'nosti dannykh v blokcheine [Economic aspects of improving data privacy in the office]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 14 (11A), pp. 451-458. DOI: 10.34670/AR.2024.52.75.050

Keywords

Zero knowledge proof (zkp), full homomorphic encryption (fhe), blockchain, cryptography, anonymity, encryption, smart contracts

References

1. Aisultan B.A. On the problem of defining the boundaries of the design of territorial planning documents // Student Bulletin. 2022. No. 46-7 (238). pp. 21-22.
2. General plan of the Shpakovsky Ministry of Defense, 2023.
3. Li A.R., Nesterov V.N. Forecasting potential risks of urban development in the tasks of strategic and territorial planning // Sysoev O.E. and others. Proceedings of the scientific and practical International Conference "Regional aspects of the development of science and education in the field of architecture, construction, land management and cadastre at the beginning of the third millennium". Komsomolsk-on-Amur, 2022. pp. 189-192.
4. Sorokina V.A. Urban planning policy of territorial development management on the example of a Small Northern city // Collection of scientific articles on materials and the International scientific and practical Conference "Socio-economic problems and prospects of territorial development". 2016. Pp. 67-70.
5. Egamberdieva, M.M., Tashtayeva, S.K., Rakhmanov, B.B. Territorial features of urbanization and urban development in Uzbekistan // Actual problems of humanities and natural sciences. 2017. No. 6-2. pp. 93-96.
6. Balchin P., Roden M. Housing policy: an introduction. – Routledge, 2019.
7. Clapham D. Housing theory, housing research and housing policy // Housing construction, theory and society. – 2018. – Vol. 35. – No. 2. – pp. 163-177.
8. Lowe S., Lowe S. Analysis of housing policy. – Macmillan Education, Great Britain, 2004. pp. 1-33.
9. Lund B. Understanding Housing Policy //Understanding Housing Policy. – Policy Press, 2017. pp. 1-22.
10. Samygin D.Yu., Baryshnikov N.G. Strategic planning of the agri-food sector: sectoral and territorial aspects // Morrisville. 2023.