УДК 316.776:004.58

Дослідження методів та розробка рекомендацій щодо застосування технології блокчейну для забезпечення безпеки та цілісності даних в мережах

Макар Кордилевський[0009-0006-5426-3430]
Андрій Аносов[0000-0002-2973-6033]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. Робота досліджує підходи до використання блокчейну як шару довіри поверх традиційних баз даних у веб-додатках. Показано, як за допомогою розподіленого реєстру можна забезпечити криптографічну незмінність критичних записів, відтворюваний аудит операцій та контроль доступу без єдиного центру довіри. Розглянуто інтеграційні патерни з ORM та журналами змін, анкеринг гешів у приватні й консорціумні мережі, а також компроміси між продуктивністю, затримками та приватністю. Сформульовано узагальнені рекомендації з впровадження блокчейну у типові архітектури веб-сервісів.
Ключові слова: blockchain, database integrity, web security, audit trail, data anchoring, smart contracts, zero-trust.

The Study of Methods and Recommendation for Applying Blockchain Technology to Ensure Data Security and Integrity in Networks

Makar Kordylevskyi[0009-0006-5426-3430]
Andrii Anosov[0000-0002-2973-6033]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. The paper explores approaches to using blockchain as a trust layer on top of traditional databases in web applications. It demonstrates how a distributed ledger can provide cryptographic immutability of critical records, reproducible auditing of operations, and access control without a single point of trust. The work considers integration patterns with ORM and change logs, anchoring of hashes in private and consortium networks, as well as trade-offs between performance, latency, and privacy. Generalized recommendations are formulated for introducing blockchain into typical web-service architectures.
Keywords: blockchain, database integrity, web security, audit trail, data anchoring, smart contracts, zero trust.

Вступ

Веб-системи покладаються на бази даних для зберігання транзакцій і подій, проте класичні механізми не забезпечують криптографічної незмінності історії в умовах багатосторонньої взаємодії. Технологія блокчейну як розподілений журнал із хеш-ланцюжком і механізмами консенсусу дає змогу фіксувати стани та зміни так, щоб будь-

яку підміну можна було виявити. Інтеграція блокчейну поверх бази даних формує перевірюваний слід змін і зменшує ризики постфактум-редагування записів, підсилюючи мережеву модель нульової довіри.

Методи

Виконано теоретичний аналіз криптографічних механізмів і моделей консенсусу, порівняння приватних і консорціумних блокчейн-платформ для корпоративних сценаріїв, формалізацію інтеграційних підходів між рівнем БД та смартконтрактами. Розглянуто варіанти збереження первинних даних поза ланцюгом із анкерингом гешів, а також схеми керування ідентичностями та ролями для перевірюваного доступу.

Таблиця 1. Підходи інтеграції блокчейну поверх бази даних для веб-систем

Метод/Підхід	Короткий опис	Переваги	Недоліки
Анкеринг гешів записів БД у блокчейн	Для кожної критичної транзакції/зміни в БД обчислюється геш і періодично фіксується в блокчейні.	Криптографічна незмінність; легка інтеграція; низькі on-chain витрати.	Потребує надійного off-chain зберігання; перевірка вимагає доступу до джерела.
Мерклеве дерево для партій змін (batch anchoring)	Геші багатьох змін агрегуються у Merkle root, який анкериться в блокчейн.	Масштабованість; менше транзакцій у ланцюгу; швидка перевірка окремих змін.	Потрібні Merkle-докази та їх зберігання; складніша реалізація.
Інтеграція через ORM/CDC (Change Data Capture)	Автоматичне перехоплення змін у БД та надсилання подій у блокчейн або шлюз аудиту.	Мінімальні зміни бізнес-логіки; узгодженість із транзакціями БД.	Залежність від СУБД/ORM; потреба в буферах та ретраях.
Приватний/консорціумний блокчейн (Fabric/Quorum)	Контрольований доступ і мережа учасників організацій.	Керованість; гнучкі політики доступу; вища продуктивність, ніж у публічних мережах.	Адміністрування й онбординг; початкові припущення довіри.
Смартконтракти для політик і аудиту	Формалізація правил зміни станів і реєстрації подій.	Прозорість; автоматизований аудит; перевірювані правила.	Ризик помилок у логіці контрактів; складність тестування.
Zero-knowledge докази (ZK)	Підтвердження коректності	Підсилення приватності; відповідність	Високі обчислювальні витрати;

	операції без розкриття даних.	регуляторним вимогам.	складність впровадження.
Гібрид: off-chain дані + on-chain індекси	Первинні дані поза ланцюгом; у ланцюгу — геші/посилання.	Баланс продуктивності й незмінності; гнучкість зберігання.	Складність синхронізації посилань; ризики доступності зовнішніх сховищ.

Результати

Підвищення цілісності даних. Блокчейн як шар незмінного аудиту зменшує ризик непомітної постфактум-редакції критичних записів. Криптографічне анкерування гешів дозволяє виявляти спроби фальсифікації через невідповідність доказів або розбіжність у Merkle-коренях. Відтворюваний і масштабований аудит. Формалізовані смартконтрактами політики прискорюють внутрішні та зовнішні перевірки, забезпечуючи прозорість процедур. За наявності CDC/ORM і батч-анкерингу трудовитрати на верифікацію історії змін можуть знижуватися орієнтовно на 30–60% залежно від покриття та частоти анкерингу. Надійне часове штампування та доказ існування. Фіксація подій у ланцюзі підтверджує момент їх існування без потреби довіри до окремого адміністратора. Треті сторони (консорціумні учасники, аудитори) можуть незалежно перевіряти коректність часових позначок і пов’язаних доказів. Баланс продуктивності та приватності. Гібридні схеми зі зберіганням первинних даних off-chain та індексацією on-chain скорочують операційні витрати, зберігаючи доказову базу. Для чутливих полів доречно застосовувати zero-knowledge докази, що підтверджують коректність без розкриття змісту. Керованість доступом і міжорганізаційна взаємодія. Консорціумні мережі з чіткими політиками доступу дають змогу безпечно обмінюватися доказами між підрозділами та організаціями, знижуючи потребу у взаємній довірі завдяки криптографічно перевірюваним подіям. Операційна спостережуваність і форензіка. Завдяки незмінному журналу подій інциденти розслідуються швидше: видно, хто і коли змінив конфігурацію, як розгортались події, і які артефакти це підтверджують. Форензік-звіти збираються без ручного “полювання” за логами з різних систем. Узгодженість конфігурацій і релізів. Коли схеми БД, міграції та політики анкеряться в ланцюзі, кожен реліз має чітко підтверджуваний склад. Командам простіше відкотитися до відомого стану, відстежити різницю між версіями і довести, що в продакшн потрапило саме те, що пройшло перевірки. Підвищення довіри між сторонами. Записи в блокчейні знімають багато питань щодо “кому вірити”. Підрядники, партнери чи внутрішні підрозділи опираються на однакові, перевірювані події, тому узгоджувати правила взаємодії та відповідальності стає значно простіше. Відповідність регуляціям і аудитам. Походження даних і їх незмінність підтверджуються стандартними доказами, тому підготовка до аудитів скорочується. Аудитори отримують прозору картину: що, коли і за якими правилами відбувалося з даними.

Обговорення

Результати пропонують практичну схему блокчейн-аудиту над БД (анкеринг гешів, Merkle-батчі, CDC/ORM, приватні/консорціумні мережі, ZK), однак переважно концептуальну: бракує експериментів із затримками, пропускною здатністю, вартістю і операційними накладними. Декларований виграш аудиту 30–60% слід верифікувати для

реальних профілів навантаження. Доданий шар ускладнює операції (шлюзи, сховище доказів, KMS) і створює ризики FP при міграціях схем, неповному CDC, а також витоки метаданих. Рекомендовано стартувати з мінімального анкерингу та мікробатчів, асинхронних конвеєрів, підписаних снапшотів, HSM/MPC і ZK для чутливих полів, профілювати параметри мережі й забезпечити DR/георезервування.

Висновки

Доцільно застосовувати блокчейн як довірений шар аудиту над базами даних у веб-сервісах, де критичні незмінність, простежуваність і перевірюваність операцій. Рекомендовано обирати приватні або консорціумні рішення, використовувати анкеринг гешів для зниження навантаження, формалізувати політики в смартконтрактах і інтегруватися з наявними засобами журналювання та керування ідентичностями. Подальші дослідження варто спрямувати на оптимізацію продуктивності анкерингу, застосування конфіденційних обчислень та автоматизацію перевірок відповідності.

Джерела

1. UDC Consortium. (2025). Universal Decimal Classification. https://udcsummary.info/php/index.php?tag=0&lang=uk&pr=Y

2. Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-project solutions for building an authorization system based on the zero trust concept. Cybersecurity: Education, Science, Technique, 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

3. DOI Foundation. (2024). DOI Citation Formatter. https://citation.doi.org/

4. Котов, К. Р. (2024). Застосування блокчейн технологій у формуванні безпеки електронного документообігу. Вінниця.

5. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства. Кібербезпека: освіта, наука, техніка, 1(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233

6. Власенко, Д. М. (2024). Дослідження технологій блокчейн для забезпечення безпеки даних та цифрових транзакцій. Запоріжжя.

7. Охрімчук, Є. І. (2020). Удосконалення фінансово економічного сектору України шляхом впровадження технології блокчейн. Суми.

8. Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). Особливості реалізації мережевих атак через TCP/IP-протоколи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915

9. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology Beyond bitcoin. Applied Innovation Review, 2, 6–19. https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

10. Androulaki, E., et al. (2018). Hyperledger Fabric A Distributed Operating System for Permissioned Blockchains. Proceedings of the Thirteenth EuroSys Conference, 30, 1–15. https://doi.org/10.1145/3190508.3190538

11. Цехмейстер, Р., Платоненко, А., Ворохоб, М., Черевик, В., & Семеняка, С. (2025). Дослідження методів забезпечення інформаційної безпеки у віртуальному середовищі. Кібербезпека: освіта, наука, техніка, 3(27), 63–71. https://doi.org/10.28925/2663-4023.2025.27.703