БЛОКЧЕЙН ДЛЯ ПРОЗОРОСТІ У СПОРТИВНИХ ЗМАГАННЯХ І АНТИДОПІНГОВОМУ КОНТРОЛІ

Фощан І.А.

Кафедра комп'ютерних наук,
Харківський національний університет радіоелектроніки,
Україна

E-mail: ivan.foshchan@nure.ua

Abstract

This paper explores the application of blockchain technology as a foundation for enhancing transparency, integrity, and trust in sports competitions and anti-doping management. The study analyzes permissioned blockchain architectures, cryptographic mechanisms such as Zero-Knowledge Proofs, and integration pathways with existing systems like ADAMS. A multi-layered conceptual model is proposed, enabling decentralized data governance, automated auditing, and secure information exchange between WADA, laboratories, and national agencies. The paper highlights the advantages of immutable data records, reduced administrative errors, and improved accountability throughout the testing lifecycle. Additionally, it addresses legal and ethical challenges, including GDPR compliance and data privacy. The findings demonstrate that blockchain-based infrastructures can serve as a technological backbone for a global ecosystem of fairness in sport, ensuring verifiable trust and resilience against data manipulation.

Вступ

Проблема допінгу у спорті залишається глобальним викликом, який підриває принципи чесної гри, довіру до результатів змагань і репутацію спортсменів. Попри роботу Всесвітнього антидопінгового агентства (WADA) та впровадження централізованих систем, таких як ADAMS, випадки втрати, спотворення чи несанкціонованого доступу до даних продовжують виникати [4]. Однією з головних проблем є централізація, коли контроль над інформацією зосереджений у вузькому колі організацій.

Блокчейн як технологія розподіленого реєстру має потенціал радикально змінити підхід до обліку, перевірки та зберігання даних у спортивній галузі. Завдяки своїм властивостям – незмінності, прозорості та децентралізації – блокчейн може стати технічною основою для систем, які забезпечують довіру навіть між сторонами, що не повністю довіряють одна одній [1], [2].

Історія розвитку технології блокчейн

Блокчейн уперше з'явився у 2008 році з публікацією Вайтпейпера Сатоші Накамото для системи Bitcoin. Початково ця технологія була спрямована на вирішення проблеми подвійного витрачання (double spending) у децентралізованих фінансових мережах. Проте згодом концепція розподіленого реєстру стала застосовуватись у значно ширшому контексті – від логістики до управління цифровими ідентичностями [8].

Починаючи з 2015 року, із запуском платформи Ethereum, блокчейн перетворився на універсальну середу для створення смарт-контрактів – автономних програм, які автоматично виконують умови угоди між сторонами. Це відкрило можливість розробки систем перевірки, сертифікації та відстежування у сферах охорони здоров'я, освіти, державного управління тощо [1], [2].

У корпоративному секторі активно розвиваються permissioned-рішення – Hyperledger Fabric, Quorum, Corda – які орієнтовані на приватні або консорціумні мережі з контрольованим доступом до даних. Такі рішення стали основою для проектів у банківській сфері, постачанні медикаментів, аграрній логістиці, а останніми роками – у спортивній аналітиці [5], [8].

У спортивній галузі блокчейн спочатку використовували переважно для токенізації квитків, продажу NFT-колекцій, захисту від фальсифікації фан-сувенірів і створення внутрішніх токенів

клубів (fan tokens). Наприклад, клуби «Барселона» та «ПСЖ» вже з 2022 року використовують blockchain-платформи Socios.com для управління фанатськими голосуваннями [9].

Однак останні дослідження вказують, що потенціал блокчейну виходить далеко за межі маркетингу – він може слугувати механізмом забезпечення прозорості та аудиту у спортивних процесах, зокрема у сфері антидопінгового контролю [2], [5]. Саме використання permissioned-архітектур (із дозволеним доступом) робить можливим створення приватних мереж, де беруть участь лише уповноважені організації: WADA, NADO, лабораторії, дисциплінарні комітети та міжнародні федерації. Такий підхід дозволяє поєднати переваги розподіленої системи з юридично контрольованими механізмами безпеки.

Крім того, сучасні дослідження (зокрема роботи Bucea-Manea-Ţoniş, 2025 [7] та López-Carril, 2025 [5]) демонструють, що блокчейн може використовуватись не лише для зберігання даних, а й для протоколювання ланцюгів дій у реальному часі, що є критично важливим для контролю за пробами, звітами й аналітичними записами. Таким чином, історія розвитку технології поступово рухається від фінансових інструментів до систем довіри та відповідальності, де спорт і медицина стають новими ключовими напрямами її впровадження.

Аналіз існуючих рішень

У наукових роботах Pinto et al. (2022) [1] та Berkani et al. (2024) [2] детально описано концепції permissioned-блокчейнів для антидопінгових систем. Їх результати показують, що така інфраструктура здатна забезпечити незмінність записів і повну відстежуваність життєвого циклу проб спортсменів – від моменту відбору до архівування результатів. Завдяки консенсусним алгоритмам типу PBFT (Practical Byzantine Fault Tolerance) і PoA (Proof of Authority), мережа може працювати швидко та без значних енергетичних витрат, що робить її придатною для інституційного використання у сфері спорту.

Дослідження Bucea-Manea-Ţoniş (2025) [7] також вказує, що блокчейн у спортивній галузі має найвищий потенціал саме в контексті аналітики допінгових перевірок, а не в комерційних застосуваннях. У статті описано модель “Blockchain for Sport Integrity”, де система реєструє всі транзакції, пов’язані з тестуванням, у вигляді криптографічно захищених записів. Таким чином, навіть якщо лабораторія або агентство спробують змінити дані заднім числом, це буде легко виявити завдяки хеш-ланцюгу подій.

Згідно зі звітом International Testing Agency (ITA) [6], лише у 2024 році зібрано понад 44 400 проб, що створює суттєве навантаження на централізовані бази даних. Крім того, ITA повідомляє про понад 120 випадків затримок у верифікації результатів, спричинених технічними або адміністративними помилками. Це підтверджує необхідність створення децентралізованої, прозорої інфраструктури, здатної автоматично фіксувати кожен етап роботи з пробами [6], [8].

Окрім академічних концепцій, у світі вже існують пілотні ініціативи. Наприклад, проект Sportchain у Нідерландах (2023) [10] використовує permissioned-блокчейн на базі Hyperledger для зберігання даних про результати тестів з легкої атлетики. Система дозволяє обмеженим користувачам (тренерам, лікарям, комісіям) перевіряти справжність даних без доступу до персональної інформації спортсменів. Аналогічні підходи досліджуються у Франції (проєкт FairPlay Ledger, 2024) [11], де блокчейн інтегрується з національними медичними базами через API.

ZK-технології (Zero-Knowledge Proofs), зокрема zk-SNARKs і zk-STARKs, надають можливість підтверджувати правильність аналізів без розкриття приватних даних спортсмена [3]. Це особливо важливо у випадках, коли доступ до результатів мають різні організації з різних країн. Наприклад, робота Lavin et al. (2024) [3] демонструє, що завдяки ZK-підходам можна зменшити ризик витоку конфіденційних медичних даних на 70% у порівнянні з традиційними цифровими системами обміну.

Крім того, дослідження Nguyen & Meijer (2024) [12] пропонує використання блокчейну не лише для реєстрації результатів, а й для аудиту процесів транспортування зразків (chain-of-custody). Автори моделюють систему, у якій кожна передача проби супроводжується смарт-контрактом, що автоматично фіксує час, підпис відповідальної особи та статус зберігання. Це значно знижує ризик фальсифікацій під час перевезення проб на міжнародному рівні.

Загалом, аналіз існуючих публікацій і пілотних проєктів свідчить, що технології permissioned blockchain у поєднанні з криптографічними доказами можуть стати основою для створення міжнародної антидопінгової екосистеми, яка поєднує прозорість, швидкість обробки даних і захист приватності. Водночас питання стандартизації форматів даних, юрисдикційних обмежень і взаємодії між агентствами залишаються відкритими [1], [2], [7], [8], [11], [12].

Архітектура блокчейн-системи антидопінгу

Система будується як permissioned (консорціумний) блокчейн з чітким розподілом ролей між учасниками: WADA, NADO, акредитовані лабораторії, міжнародні федерації, незалежні аудитори та (за потреби) національні органи влади. Така модель поєднує контроль доступу корпоративних мереж із властивостями незмінного журналу (audit trail) – підхід рекомендований у [1], [2], [7], [9].

Архітектура логічно поділяється на шари, які представлені в табл. 1.

Табл. 1. Структура архітектурного підходу (high-level)

№ з/п	Шар	Опис
1	Клієнтський шар (Client / UI)	мобільні додатки для офіційного відбору проб, веб-інтерфейси для лабораторій, портали для аудиторів і спортсменів (обмежений доступ)
2	API / Integration layer	шлюзи для інтеграції з ADAMS, лабораторними LIMS, ERP та медичними системами
3	Blockchain layer (consortium)	валідаторні вузли, смарт-контракти, меркл-структури, механізми консенсусу (PBFT/PoA та їх варіанти)
4	Off-chain storage	захищені сховища для бінарних звітів, великих файлів та персональних даних (зашифровані S3-сховища або приватні IPFS/Storj), з наданням CIDs/хешів у блокчейн
5	Security & Privacy services	PKI / DID, HSM / KMS для управління ключами, ZK-proof сервіс, модулі шифрування і аудит-журналів
6	Monitoring / Ops / Auditing	SIEM, метрики, інструменти аудиту та незалежні перегляди безпеки

Багаторівнева архітектура блокчейн-системи, створена для підвищення прозорості антидопінгових процесів у спорті (рис. 1), відображає основні компоненти: клієнтський рівень (додатки для збору проб), інтеграційний шар (взаємодія з ADAMS і лабораторними системами), блокчейн-консорціум із вузлами-валідаторами та смарт-контрактами, офчейн-сховище для зашифрованих даних, а також сервіси безпеки й приватності (PKI, DID, ZK-proofs).

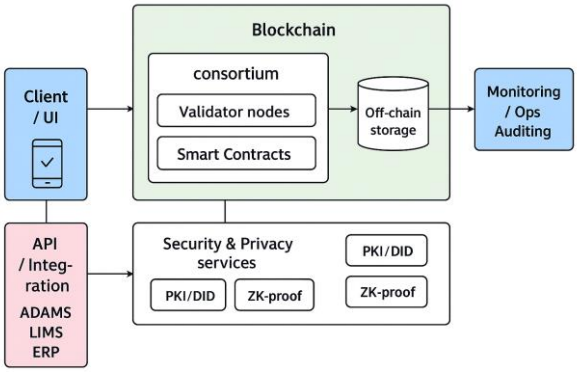

Рис. 1. Архітектура permissioned-блокчейну для антидопінгового контролю

При цьому можна виділити такі ролі вузлів і права доступу.

1. Валідаційні (validator/consensus) вузли – керують консенсусом і мають право підписувати блоки; керуються WADA, кількома великими NADO та провідними лабораторіями. (PBFT/PoA рекомендується для низької латентності та детерміністичності [1], [2].)

2. Узлові спостерігачі (observer nodes) – національні федерації та комітети можуть запускати read-only вузли для перевірки журналів.

3. Клієнтські вузли / light clients – мобільні/термінальні пристрої, що підписують транзакції, але не зберігають повного ланцюгу.

4. Аудиторські вузли – незалежні організації, що мають розширені права на запити та детально переглядати метадані (з дотриманням приватності).

5. Revocation & Governance – окремий модуль/комітет для управління додаванням/видаленням вузлів, ролей та політик доступу (on-chain governance контракт).

В життєвому циклі даних можна виділити кілька ключових об'єктів.

1. SampleID (унікальний ідентифікатор проби). На момент відбору генерується SampleID; створюється криптографічний хеш усіх первинних метаданих (salted hash) – цей хеш записується в блокчейн [1, 11].

2. On-chain транзакція (event record) – мінімальний набір полів (зберігаються як JSON-подібна структура або в полях транзакції):

1) sampleHash – хеш метаданих або CID на off-chain файл;

2) eventType – {collection, transfer, receipt, analysis_requested, analysis_completed, dispute_opened, judgment};

3) actorID – DID/PKI ідентифікатор суб'єкта, що підписав подію;

4) timestamp – UTC ISO8601;

5) prevEventHash – для зв'язності ланцюга custody;

6) signature – цифровий підпис від actorID.

3. Off-chain артефакти – PDF-звіт лабораторії, BLOBs, відео/фото збору проби; для них зберігається лише CID / хеш у блокчейні, а самі файли – в зашифрованому сховищі.

Механізми приватності та криптографії передбачає застосування різник компонентів. Hashing & Commitments, коли всі персональні/чутливі дані хешуються і тільки хеш/commit записується on-chain [3]. Off-chain шифрування забезпечує шифрування симетричним ключем (AES-GCM), ключі зберігаються у розподіленому KMS/HSM; доступ надається через смарт-контракти після перевірки прав. Zero-Knowledge Proofs (ZK-proofs) застосовуються для доведення властивостей без розкриття – наприклад: «результат відповідає межам допустимого» або «аналіз проведено в сертифікованій лабораторії» без передачі особистих даних [3]. Рекомендуються zk-SNARKs/zk-STARKs для селективного розкриття. Merkle Trees використовується для оптимізації зберігання і перевірок великих наборів подій (наприклад пакети подій за добу) – у блоці зберігається корінь дерева, а деталі можна доказати через Merkle proof. Використання Decentralized Identifiers (DID) або сертифікатів X.509 для ідентифікації учасників і підписування подій. HSM для зберігання приватних ключів у вузлах лабораторій і NADO.

Але незважаючи на значний потенціал, існують обмеження щодо використання блокчейн-систем серед яких можна виділити наступні аспекти: юридичні ризики (колізія між незмінністю даних та GDPR), масштабованість (необхідність ефективних консенсусів PBFT/PoA), довіра між учасниками (потреба політичної згоди), захист метаданих (ризик кореляції за часовими мітками) [3, 4]. Також критично важливими можуть бути питання згоди спортсменів, збереження конфіденційності медичних даних і механізми оскарження результатів. Тому рекомендується створення незалежних наглядових комітетів для моніторингу доступу до даних і дотримання етичних стандартів.

Використання технології блокчейн у сфері антидопінгового контролю здатне суттєво підвищити довіру до спортивних результатів і забезпечити прозорість усіх процесів. Поєднання технічних інновацій (permissioned blockchain, ZK-proofs) та юридичної адаптації створює основу для побудови глобальної системи чесності у спорті. [1], [2], [3]

Висновки

Проведене дослідження підтвердило, що впровадження блокчейн-технологій у сферу антидопінгового контролю може стати ключовим елементом формування нової моделі довіри у спорті. Завдяки властивостям незмінності, децентралізації та криптографічного захисту даних, блокчейн здатен усунути одну з головних проблем сучасних систем – централізований контроль над інформацією та ризик її маніпуляцій. Консорціумна (permissioned) архітектура, побудована на принципах розподіленого управління, дозволяє поєднати відкритість для перевірки з чітким контролем доступу, що відповідає вимогам міжнародних організацій, таких як WADA та ITA.

Використання механізмів смарт-контрактів забезпечує автоматизацію основних етапів життєвого циклу проб – від моменту відбору до публікації результатів, мінімізуючи людський фактор і можливість навмисних або випадкових помилок. Додаткове застосування технологій нульового розголошення дозволяє забезпечити баланс між прозорістю процесів та захистом персональних медичних даних спортсменів, що є критично важливим з огляду на вимоги етичних норм і GDPR.

Досліджена концептуальна архітектура системи демонструє, що інтеграція блокчейну з існуючими платформами (зокрема ADAMS) є технічно можливою через створення інтеграційних шлюзів та використання офчейн-сховищ. Такий підхід забезпечує масштабованість системи, сумісність із поточними стандартами й поступовий перехід без порушення поточних операційних процесів антидопінгових агентств. Описана модель передбачає використання децентралізованих ідентифікаторів (DID), журналів аудиту, криптографічного підпису подій та меркл-структур для перевірки достовірності даних, що підвищує рівень контролю та надійності всієї екосистеми.

Водночас дослідження показало низку викликів, які потребують подальшого опрацювання. Серед них – юридичні колізії між принципом незмінності даних у блокчейні та вимогами до їх можливого видалення відповідно до GDPR, складність міжнародної стандартизації форматів даних, а також необхідність створення наднаціональних механізмів управління та сертифікації учасників мережі. Не менш важливим аспектом є розроблення етичних і правових процедур щодо доступу до інформації, забезпечення добровільної згоди спортсменів та регулювання питань відповідальності сторін.

Отже, використання блокчейну у сфері антидопінгового контролю відкриває нову парадигму взаємодії між органами контролю, лабораторіями та спортивними федераціями. Така система здатна забезпечити повну відстежуваність і перевірюваність усіх процесів, зменшити адміністративні витрати, підвищити ефективність перевірок і значно зміцнити довіру суспільства до результатів спортивних змагань. У перспективі реалізація подібних систем може стати фундаментом для формування глобальної «екосистеми чесності у спорті», де технологічна надійність підкріплює етичні принципи рівності, відкритості та справедливості.

Література

1. Pinto, F. Blockchain for doping control applications in sports: a conceptual approach / F. Pinto, Y. Rahulamathavan, J. Skinner // Future Internet. – 2022.

2. Berkani, A. S. Blockchain use cases in the sports industry: a systematic analysis / A. S. Berkani [та ін.]. – Palgrave/Springer, 2024.

3. Lavin, R. A survey on the applications of zero-knowledge proofs / R. Lavin, X. Liu, H. Mohanty [та ін.] // arXiv. – 2024.

4. ADAMS (Anti-Doping Administration and Management System) [Електронний ресурс] / World Anti-Doping Agency (WADA). – Режим доступу: https://www.wada-ama.org/en/what-we-do/adams (дата звернення: 22.10.2025).

5. Principe, V. Transformative blockchain technological approaches to sports events / V. Principe, T. Ribeiro, S. López-Carril // Frontiers in Sports and Active Living. – 2025.

6. 2024 Operational Figures Report [Електронний ресурс] / International Testing Agency (ITA). – Режим доступу: https://ita.sport/news/the-international-testing-agency-publishes-2024-operational-figures (дата звернення: 22.10.2025).

7. Bucea-Manea-Ţoniş, R. Blockchain in sports: a comparative analysis / R. Bucea-Manea-Ţoniş // Applied Sciences. – 2025.

8. Casino, F. A systematic literature review of blockchain-based applications: current status, classification and open issues / F. Casino, T. K. Dasaklis, C. Patsakis // Telematics and Informatics. – 2019. – Т. 36. – С. 55 – 81.

9. Morabito, V. Business innovation through blockchain: the B3 perspective and emerging use cases. – Springer, 2022.

10. Van der Meer, J. Sportchain: applying blockchain in sports data integrity / J. Van der Meer, E. Koelman // IEEE Access. – 2023.

11. Dupont, C. FairPlay Ledger: blockchain-based anti-doping infrastructure in France / C. Dupont, A. Lemoine // Journal of Sports Integrity. – 2024.

12. Nguyen, P. T. Blockchain-based chain-of-custody for biological samples in global sports / P. T. Nguyen, R. Meijer // Future Internet. – 2024.