DOI: 10.34185/1991-7848.itmm.2025.01.111

СИСТЕМА БАГАТОРІВНЕВОЇ ВЕРИФІКАЦІЇ ПЕРСОНАЛЬНИХ ДАНИХ У БЛОКЧЕЙН-СЕРЕДОВИЩІ

Ситник Р.С.[1], Гнатушенко Вік.В.[1,2]

[1]*Український державний університет науки і технологій, Україна*

[2]*Національний технічний університет «Дніпровська політехніка», Україна*

Анотація. *У роботі запропоновано інноваційний підхід до вирішення проблеми верифікації та захисту персональних даних у системах на основі технології блокчейн. Розроблено метод забезпечення достовірності та цілісності даних, що базується на математичній моделі з використанням комплексної функції валідації та ієрархічної структури вузлів верифікації. Запропонована модель представляє кожен елемент даних як кортеж компонентів, що включає версію даних, цифровий підпис джерела, часову мітку, геш попередньої версії та метадані верифікації. Достовірність оцінюється через інтегральний показник, що враховує різні аспекти валідації. Впроваджено систему "довірених джерел" з динамічним оновленням рівня довіри на основі історії операцій та алгоритму консенсусу Proof-of-Authority. Архітектурно система реалізується через створення ієрархічної структури вузлів верифікації, де кожен рівень відповідає за певний аспект перевірки даних. Запропоноване рішення забезпечує баланс між захистом даних та зручністю їх використання.*

Ключові слова: *блокчейн, персональні дані, цілісність даних, криптографічний захист, смарт-контракти, цифрова безпека.*

В епоху цифровізації та експоненційного зростання об'ємів даних проблема захисту персональної інформації набуває критичного значення для суспільства. Технологія блокчейн, завдяки своїм фундаментальним властивостям незмінності та розподіленості, представляє значний потенціал для вирішення цієї проблеми. Проте, застосування блокчейну для обробки персональних даних створює низку специфічних викликів, пов'язаних із забезпеченням їх достовірності та цілісності в умовах розподіленої архітектури, а також із необхідністю дотримання вимог законодавства щодо захисту персональних даних [1]. Традиційні методи захисту інформації виявляються недостатньо ефективними через особливості блокчейн-систем та специфіку роботи з персональними даними, що вимагає розробки спеціалізованих підходів.

Аналіз останніх досліджень у сфері безпеки блокчейн-систем, виявляє значний прогрес у розвитку загальних механізмів криптографічного захисту та методів верифікації даних у розподілених системах [2]. Водночас, питання інтеграції цих механізмів із вимогами законодавства про захист персональних даних, зокрема забезпечення права на забуття та можливості модифікації даних без порушення цілісності блокчейну, залишаються недостатньо вирішеними [3]. Саме на подолання цих обмежень спрямоване ця робота.

В основу запропонованого підходу покладено математичну модель оцінки достовірності персональних даних у розподіленій блокчейн-системі. Ключовою інновацією є представлення кожного елементу даних D як кортежу (V, S, T, H, M), де V - версія даних, S - цифровий підпис джерела, T - часова мітка, H - хеш попередньої версії, M - метадані верифікації.

Достовірність даних оцінюється через комплексну функцію валідації:

$$F(D) = \alpha_1 V(S) + \alpha_2 T(H) + \alpha_3 C(M), \quad (1)$$

де V(S) – функція верифікації цифрового підпису, T(H) – функція перевірки цілісності ланцюжка версій, C(M) – функція валідації метаданих, а α_1, α_2, α_3 – вагові коефіцієнти.

Інтегральний показник достовірності розраховується як:

$$R = F(D) \times \Pi(1 - P_i), \quad (2)$$

де P_i – ймовірність компрометації і-го рівня верифікації. Цей показник знаходиться в діапазоні [0,1], де R = 1 означає максимальну достовірність даних, а R = 0 – повну недостовірність. Такий підхід дозволяє комплексно оцінювати надійність персональних даних з урахуванням різних аспектів їх верифікації.

Архітектурно система реалізується через створення ієрархічної структури вузлів верифікації, де кожен рівень відповідає за певний аспект перевірки даних. Перший рівень забезпечує базову валідацію форматів та перевірку відповідності схемам, другий – криптографічну верифікацію цифрових підписів та повноважень джерела, а третій – складні механізми перехресної перевірки та узгодження з існуючими записами. Така структура забезпечує надійність системи та її стійкість до різних типів атак.

Важливим концептуальним елементом є система "довірених джерел" – спеціально авторизованих вузлів мережі з правом внесення та модифікації

персональних даних, робота за алгоритмом консенсусу Proof-of-Authority [4]. Кожен такий вузол характеризується власним рівнем довіри, який динамічно оновлюється на основі історії операцій, що забезпечує додатковий рівень захисту від несанкціонованого доступу.

Система включає механізм версіонування даних на основі деревовидної структури, що дозволяє зберігати повну історію змін та підтримувати паралельні гілки модифікацій. Важливим елементом є система керування доступом на основі розширеної рольової моделі, яка враховує не лише ролі користувачів, але й додаткові атрибути та контекст операцій, що забезпечує гнучкі політики доступу до персональних даних.

Висновки: Запропонований метод забезпечення достовірності та цілісності персональних даних у блокчейн-системі є комплексним рішенням, що враховує як технічні аспекти захисту інформації, так і нормативні вимоги до обробки персональних даних. Ключовими перевагами методу є модель оцінки достовірності даних, ієрархічна система верифікації, механізми диференційованого доступу та контролю за використанням даних.

Практична цінність дослідження полягає у можливості застосування розробленого методу для створення захищених інформаційних систем обробки персональних даних у різних сферах, включаючи державні реєстри, медичні інформаційні системи, фінансові установи та комерційні організації. Особливо актуальною є можливість забезпечення балансу між захистом даних та зручністю їх використання, що досягається через впровадження гнучких механізмів управління доступом та автоматизованих процесів верифікації.

Подальший розвиток методу передбачає вдосконалення механізмів автоматизації процесів верифікації, розширення можливостей інтеграції з різними інформаційними системами та розробку додаткових інструментів аналізу й моніторингу для підвищення ефективності виявлення потенційних загроз. Також планується дослідження можливостей застосування запропонованого підходу в контексті нових технологічних трендів, таких як Інтернет речей та граничні обчислення, що створює перспективи для

подальшого підвищення рівня захисту персональних даних в умовах цифрової трансформації суспільства.

ЛІТЕРАТУРА

1. Sim, W. L., Chua, H. N., & Tahir, M. (2019, November). Blockchain for identity management: The implications to personal data protection. In 2019 IEEE Conference on Application, Information and Network Security (AINS) (pp. 30-35). IEEE. DOI: 10.1109/AINS47559.2019.8968708
2. Singh, S., Hosen, A.S. and Yoon, B., 2021. Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access, 9, pp.13938-13959. DOI: 10.1109/ACCESS.2021.3051602
3. Tatar, U., Gokce, Y. and Nussbaum, B., 2020. Law versus technology: Blockchain, GDPR, and tough tradeoffs. Computer Law & Security Review, 38, p.105454. DOI: 10.1016/j.clsr.2020.105454
4. Joshi, S., 2021. Feasibility of proof of authority as a consensus protocol model. arXiv preprint arXiv:2109.02480. DOI: 10.48550/arXiv.2109.0248

Multi-level Personal Data Verification System in Blockchain Environment

Roman Sytnyk, Viktoriia Hnatushenko

Abstract. *This paper proposes an innovative approach to solving the problem of verification and protection of personal data in blockchain-based systems. A method for ensuring data reliability and integrity has been developed, based on a mathematical model using a complex validation function and a hierarchical structure of verification nodes. The proposed model represents each data element as a tuple of components including data version, digital source signature, timestamp, hash of the previous version, and verification metadata. Reliability is evaluated through an integral indicator that takes into account various aspects of validation. A system of "trusted sources" has been implemented with updating of the trust level and the Proof-of-Authority consensus algorithm. Architecturally, the system is implemented through the creation of a hierarchical structure of verification nodes, where each level is responsible for a specific aspect of data verification. The proposed solution provides a balance between data protection and ease of use.*

Keywords: *blockchain, personal data, data integrity, smart contracts, digital security.*

REFERENCE

1. Sim, W. L., Chua, H. N., & Tahir, M. (2019, November). Blockchain for identity management: The implications to personal data protection. In 2019 IEEE Conference on Application, Information and Network Security (AINS) (pp. 30-35). IEEE. DOI: 10.1109/AINS47559.2019.8968708
2. Singh, S., Hosen, A.S. and Yoon, B., 2021. Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access, 9, pp.13938-13959. DOI: 10.1109/ACCESS.2021.3051602
3. Tatar, U., Gokce, Y. and Nussbaum, B., 2020. Law versus technology: Blockchain, GDPR, and tough tradeoffs. Computer Law & Security Review, 38, p.105454. DOI: 10.1016/j.clsr.2020.105454
4. Joshi, S., 2021. Feasibility of proof of authority as a consensus protocol model. arXiv preprint arXiv:2109.02480. DOI: 10.48550/arXiv.2109.0248