1. Bogdanov A., Knudsen L., Leander G. та ін. PRESENT: An Ultra-Lightweight Block Cipher // Cryptographic Hardware and Embedded Systems – CHES 2007. Berlin : Springer, 2007. С. 450–466.
2. Wang Y., Ha Y. Compact FPGA implementation of PRESENT cipher with optimized S-box // IEEE Transactions on Very Large Scale Integration Systems. – 2011. – Vol. 19, №10. – P. 1864–1873.
3. A. Donald Keedwell and József Dénes. Latin Squares and their Applications. Elsevier, 2015. 439 с. URL: https://doi.org/10.1016/c2014-0-03412-0.

Розробка архітектури програмного застосунку для децентралізованої торгівлі електроенергією з використанням смарт-контрактів в блокчейн

УДК 004.4

Ганна Неласа[1], Вахтанг Чіхладзе[2],
Андрій Ублінських[3], Олег Неласий[4]

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова,
[1]annanelasa@gmail.com,
Національний технічний університет України «КПІ імені Ігоря Сікорського», [2]the.vaho1337@gmail.com,
Cytric, [3]andreo.ublin24@gmail.com,
Національний університет «Запорізька політехніка», [4]oleg.nelasy@gmail.com

В роботі представлено архітектуру програмного застосунку для децентралізованої торгівлі електроенергією з використанням смарт-контрактів в блокчейн [1]. На сьогодні смартконтракти набули широкого застосування та стали невід'ємною складовою блокчейн і фінансової індустрії.

Основна ідея полягає в токенізації 15-хвилинних порцій електроенергії, розділенні вартості електроенергії та прибутку на різні токени, та введенні фінансового посередника між виробниками та споживачами, який балансує момент розрахунків між ними, тобто сплачує виробнику за поставлений обсяг електроенергією відразу, а оплату від споживачів отримує пізніше при використанні відповідних порцій. Фінансовий посередник може отримувати дохід за свої послуги, оскільки протокол Pendle [2] довів створення ринку дохідності при розділенні базового активу та майбутнього доходу.

Відповідно в схемі використовуються токени:

- PT (PrincipalToken) - токен, який надає право користування електроенергією в заданий проміжок часу, «тіло» активу, тобто сума, що буде повернута після настання дати погашення. PT не приносить дохід, а лише гарантує повернення активу.
- YT (YieldToken) - токен, який містить у собі майбутній прибуток виробника-продавця.
- SY (Standardized Yield Token) виступає як «обгортка», що представляє повну вартість активу разом із майбутньою дохідністю.

Роботу виконано за держбюджетною темою «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації. Розділ 1. Організаційні та математичні моделі взаємодії учасників децентралізованого ринку електроенергії» (ЦИФРОВІЗАЦІЯ), КПКВК 6541230.

1. Evdokimov, V.; Kudin, A.; Chikhladze, V.; Artemchuk, V. A Blockchain Architecture for Hourly Electricity Rights and Yield Derivatives. FinTech. – 2026, 5(1), №2. https://doi.org/10.3390/fintech5010002
2. Pendle Finance Documentation. Available URL: https://docs.pendle.finance (application date 09.05.2026).

Гібридний метод приховування водяних знаків на основі конформних відображень та сингулярного розкладу матриць

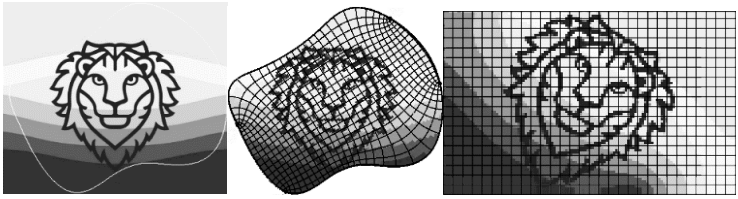
УДК 004.056.55 : 517.54

Андрій Бомба[1], Михайло Бойчура[2]

Національний університет водного господарства та природокористування, [2]m.v.boichura@nuwm.edu.ua

Традиційні методи вбудовування невидимих цифрових водяних знаків (ЦВЗ) в області є вразливими до геометричних атак, а використання частотних методів ускладнюється у випадку фігур складної геометрії. Метою роботи є підвищення захищеності зображень з криволінійною границею шляхом розроблення робастного методу вбудовування ЦВЗ, стійкого до топологічних деформацій.

Запропоновано підхід до накладання ЦВЗ на однозв'язну область (зображення) довільної форми. Він передбачає поєднання числових методів конформних відображень для перетворення досліджуваної області на прямокутник [1] та сингулярного розкладу матриць – для подальшого вбудовування прихованої інформації [2]. Окрім іншого, підхід передбачає побудову геометричного криптографічного ключа.



а) б) в)

Рис. 1. Початкове зображення (а), сітки фізичної області (б) та області комплексного потенціалу (в)

Алгоритм для вбудовування ЦВЗ складається з наступних кроків: визначаються межі криволінійної фігури, здійснюється відображення фізичної області на прямокутник, формується матриця яскравості пікселів, остання розбивається на блоки, до яких застосовуються сингулярні розклади,