НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2024»

Збірник матеріалів конференції
5 червня 2024 р.

Київ – 2024

УДК 620.9 + 349 + 004 + 003.26

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол №6 від 30.05.2024 р.)

Організаційний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Програмний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Відповідальний за випуск:
В.О. Артемчук

Usage of blockchain technologies in energetics – 2024: collection of materials of the scientific and practical conference, Kyiv, June 5, 2024, PIMEE of NAS of Ukraine. - 2024. - 36 p.

Використання блокчейн технологій в енергетиці – 2024 : збірник матеріалів науково-практичної конференції, м. Київ, 5 червня 2024 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2024. – 36 с.

ЗМІСТ

L.V. Kovalchuk, O.Y. Bespalov

USING CONSTANT PRODUCT MARKET MODEL FOR P2P "GREEN" ENERGY TRADING

One of the main questions needed to be answered in case of p2p-trading of "green" energy, is question of payments and price forming [1]. As in this case trading occurs between households in fully decentralized environment, there are no governing body which makes decision about price value.

We consider the next two main possibilities, namely two models: Order Book (OB) Model (OBM) [2] and Automated Market Maker (AMM) Model [3].

In this report we consider one variant of AMM Model, namely Constant Product Market (CPM) [4], and its application to "green" energy market. We explain what we need to change in the CPM model for such application.

Constant Product Market description.

We start with a short explanation of the Constant Product Market (CPM [3, 4]), whose functioning is defined by CMT rules. Let some liquidity pool in Constant Product Market consist of two asset, A and B, of the value a and b units, respectively, where the prices of these two assets, expressed in USD or USDT, are merely the same. Roughly speaking, the price of a units of asset A is b units of asset B, or the price of one unit of asset A is $\frac{b}{a}$ units of asset B, and vice versa. Let's define the constant T as $T = a \cdot b$.

Next, define value ρ, called ***the transaction fee***, which may be expressed as a percentages or a ratio, and value $\gamma = 1 - \rho$. Note that value ρ is rather small (for example, $\rho = 0.003$ for Uniswap), so inequality $\frac{1}{\gamma} = 1 + \frac{\rho}{1-\rho} > 1 + \rho$ may be rewritten approximately as $\frac{1}{\gamma} \approx 1 + \rho$.

Let's assume Trader wants to buy Δb units of asset B. Then the amount Δa of asset A, which he should pay for it, is defined from equation

$$(b - \Delta b)(a + \gamma \cdot \Delta a) = T,$$

or $\Delta a = \frac{a \cdot \Delta b}{\gamma (b - \Delta b)}$, which for a large enough b and a small (w.r.t. b) value of Δb may be approximated with equality

$$\Delta a \approx (1 + \rho) \cdot \frac{a}{b} \cdot \Delta b, \qquad (1)$$

using the approximation for $\frac{1}{\gamma}$ given above. Relation (1) explains why we

consider ρ a commission: if we set $\rho = 0$, we get $\Delta a = \frac{a}{b} \cdot \Delta b$, where the price of one unit of asset B is just $\frac{a}{b}$ units of asset A.

After the $\Delta a / \Delta b$ exchange, we get the new state of the market and the new value $T' > T$ of the product:

$$T' = (b - \Delta b)(a + \Delta a) = T - \Delta b \cdot a + (b - \Delta b) \cdot \Delta a = T + \Delta b \cdot a \left(\frac{1}{\gamma} - 1 \right) > T,$$

because of $0 < \gamma < 1$. So, as we can see from (8), each trade actually increases the product of asset values. Note that if we set $\rho = 0$ then the value of the product will be stable all the time after any number of trades, and this fact explains the name "Constant Product Market".

Adopting CPM to energy market.

Let us have liquidity pool with two assets, A and B. One of the assets, say A, is futures of energy selling, the other is the corresponding futures on energy buyng. In general CPM, the price of the asset A w.r.t. the asset B may tend to zero, when the amount of the asset B tends to zero. But in case of energy trading such situation is not allowed, because no trader wants to sell energy with price lower than some threshold. So we need to transform the CPM in a such way that the price can't be lower than some fixed value Γ – for example, it may be the initial trading price, set when this pool was created, or some price which is a bit lower but acceptable for energy sellers. One of the way of such modification is to use the formula

$$\Delta b = \max \left\{ \Gamma, \frac{b \cdot \Delta a}{\gamma (a - \Delta a)} \right\}$$

instead of formula

$$\Delta b = \frac{b \cdot \Delta a}{\gamma (a - \Delta a)}.$$

We investigate the obtained model for energy trading and its properties, and give detailed description of its work.

1. Bielecki, S.; Skoczkowski, T.; Sobczak, L.; Wołowicz, M. Electricity Usage Settlement System Based on a Cryptocurrency Instrument. Energies 2022, 15, 7003. https://doi.org/10.3390/en15197003
2. DeFi protocol. Available online: https://www.pcmag.com/encyclopedia/term/defi-protocol (accessed on 21 May 2023).
3. Angeris G.; Chitra T. Improved Price Oracles: Constant Function Market Makers. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT '20). Association for Computing Machinery, New York, NY, USA, 2020. 80–91. https://doi.org/10.1145/3419614.3423251
4. Handbook of ParaSwap. Available online: https://doc.paraswap.network/ (accessed on 21 May 2023).

В.М. Горбачук, Д.І. Ніколенко, М.М. Пустовойт, В.В. Годлюк, Д.О. Рибачок

СМАРТ-КОНТРАКТИ В ЕНЕРГЕТИЦІ

Однією з відмітних рис технології блокчейн є смарт-контракт – самовиконувані та програмовані угоди, закодовані в блокчейні. Такі контракти автоматизують і втілюють наперед визначені умови, скеровуючи процеси і зменшуючи потребу в посередниках. Поєднання прозорої та безпечної облікової книги (ledger) блокчейну з програмованістю смарт-контрактів сприяє ефективності трансакцій поміж різних секторів і довірі до цих трансакцій, розвиваючи ширшу концепцію технології розподіленої облікової книги (distributed ledger technology, DLT).

На традиційному ринку електрики електроенергія надходить від великих електростанцій і через національні та регіональні електромережі до місцевих розподільних систем, приєднаних до кінцевих користувачів. Оператори мереж забезпечують узгодження попиту і пропозиції та підтримують якість електрики в будь-який час. Ця якість включає забезпечення підтримання частоти енергосистеми в межах дозволеного діапазону, миттєве балансування попиту і пропозиції, існування достатньої спроможності для зберігання енергії на випадок значних непередбачуваних змін попиту чи пропозиції як допоміжної (ancillary) послуги. Операторів мереж можна вважати посередниками між виробниками і споживачами. У традиційних енергосистемах управління балансом здійснюється на рівні передачі, позаяк у сучасних мережах таке управління здійснюється на рівні локального розподілу. Швидка інтеграція переривчастої (intermittent) і часто дуже розподіленої відновлюваної генерації в енергосистему, а також інтеграція продуктів і послуг, основаних на інформаційно-комунікаційних технологіях, збільшили потребу використання інтелектуальної платформи для енергоменеджменту та балансування попиту і пропозиції. Впровадженням такої платформи є застосування розумних (smart) технічних засобів, ініціатив розумної взаємодії, інструментів розумного моніторингу (смарт-контрактів).

Смарт-контракти – це прості коди, які можна виконати для реалізації певної функції. Ці контракти еквівалентні паперовим контрактам, але усувають потребу в правоохоронному органі (enforcement agency) для забезпечення відповідності (compliance) дій сторін контракту його умовам, оскільки в разі виконання такого контракту він завершується відповідно до запланованих (запрограмованих) наслідків, незалежно від будь-якого додаткового втручання людини [1]. Відома основана на технології блокчейну екосистема вуглецевих кредитів (carbon credit), яка включає кілька смарт-контрактів: записування суттєвих даних з використанням системи реєстрів (registry system) на блокчейні, добування (mining) вуглецевих токенів, контракт з мультипідписом (multisignature), автоматизований маркетмейкер (market maker), подібний до ДП «Енергоринок» [2]. Вивчався вплив смарт-контрактів у різних розумних мережах [3–5]. Дослідження неоднорідності

споживчих переваг щодо смарт-контрактів на послуги електрики в контексті розумної мережі показує, що інтелектуальні постачальники послуг електрики можуть значно знижувати свої витрати на залучення клієнтів (customer acquisition costs), орієнтуючись на клієнтів з особливими характеристиками [6]. Якщо має місце єдиний контракт для енергоменеджменту розумного житлового будинку з фотоелектричним виробництвом, електричними транспортними засобами, системою енергонакопичення на акумуляторах (battery energy storage system), а кожний клієнт у цьому будинку має гнучкий контракт на електрику, то за допомогою оптимальної кількості законтрактованої електрики енергоагрегата та інтелектуальної системи енергоменеджменту витрати на електрику будинку загалом можна зменшити майже вдвічі [7].

Схема [8] дає децентралізоване виконання економічної диспетчеризації з використанням смарт-контрактів, забезпечує оснований на вартості репутації механізм стимулювання і багатосторонню трансакцію, основану на вартості репутації та платіжної вартості (billing value) [9]. Ця схема: сприяє розподілу надлишку енергії серед сусідніх структур, щоб зменшувати вимоги до енергопередачі у менеджменті традиційних енергомереж; може в достатній мірі гарантувати дотримання всіма залученими сторонами плану диспетчеризації; усуває потребу залучення учасників до торгів, таким чином зберігаючи час і запобігаючи конфліктам трансакцій.

Схема [10] пропонує поточний і майбутній статус торгівлі вуглецевими викидами (газами) в енергетичній галузі, вивчаючи зразки зростання та перешкоди зростанню, розробляє діаграму, що окреслює структуру процесу оптимізації для цієї торгівлі з використанням технології блокчейну та розумної системи торгівлі вуглецевими викидами, розробляє модель для смарт-контрактів у цій системі. Ця схема: підвищує безпеку й ефективність торгівлі вуглецевими викидами; поліпшує механізм зберігання даних цієї торгівлі; оцінює достовірність (credibility) учасників торгів; точно веде облік трансакцій; пропонує високий ступінь спроможностей автоматизованих розрахунків (automated settlements).

Схема [11] запроваджує інноваційну структуру смарт-контрактів у розумних містах, реалізує практичний і життєздатний динамічний протокол безпеки послуги, демонструє практичність і здійсненність (feasibility) децентралізованої архітектури безпеки послуги для різноманітних пристроїв Інтернету речей (Internet of Things, IoT). Ця схема: досліджує процес реєстрації пристроїв IoT у гетерогенних мережах; вивчає встановлення захищеного зв’язку поміж кількох гетерогенних мереж; перевіряє процедури, пов’язані з реєстрацією, комунікацією та виконанням динамічних протоколів безпеки послуг серед пристроїв IoT у гетерогенній мережі.

Схема [12] розширює децентралізовану структуру однорангового (peer-to-peer, P2P) ринку, об’єднує блокчейн-фреймворк Hyperledger Fabric із налаштованим смарт-контрактом, документує багатокроковий процес клірингу ринку (market clearing) протягом дня. Ця схема: сприяє вирізненню

продуктів через двосторонні переговори; виробляє довіру учасників і зберігає конфіденційність під час двосторонніх переговорів; вивчає вплив відмінності продуктів P2P-ринку на доходи і спрямування відновлюваної енергії.

Схема [13] пропонує ретельний аналіз досліджень смарт-контрактів з охопленням обмежень і виграшів, представляє 6-рівневу архітектуру й енергетичний смарт-контракт, проводить оцінювання різноманітних реальних застосувань смарт-контрактів у промислових контекстах і пілотних демонстраційних ініціативах. Ця схема: пропонує перспективну базу для ініціації розгортання смарт-контрактів; надає структурований опис переваг і недоліків, пов'язаних зі смарт-контрактами.

DLT є наріжним каменем систем блокчейну, істотно відрізняючись від традиційних підходів до менеджменту та верифікації даних. У сфері торгівлі вуглецевими викидами DLT пропонує децентралізовану, прозору, непорушну облікову книгу, яка сприяє ефективним і безпечним трансакціям, усуваючи потребу в посередниках. P2P-природа DLT гарантує, що записи трансакцій одночасно зберігаються поміж вузлів мережі, поліпшуючи стійку до втручання (tamper-resistant) екосистему, де кожний учасник володіє синхронізованою і неперервно оновлюваною обліковою книгою. Цей децентралізований консенсусний механізм [14] не тільки підвищує цілісність і безпеку даних, але й породжує довіру серед учасників, прокладаючи шлях для інноваційних і прозорих платформ торгівлі вуглецевими викидами.

Розподілена облікова книга є непорушним історичним записом: фактично всі трансакції блокчейну записуються у непорушну облікову книгу і розподіляються по всій мережі. Загалом виділяють 3 типи розподіленої облікової книги: облікова книга з єдиним записом (single-entry) включає односторонній запис у стовпці кредиту чи дебету; облікова книга з подвійним записом включає одночасне відстеження боргів і кредитів; облікова книга з потрійним записом включає розширену систему подвійного запису, де всі входи трансакції перевіряються та захищаються криптографічною системою. Блокчейн використовує потрійну облікову книгу, яка включає борг, кредит, зв'язки між попередніми блоками.

Енергія – це природний ресурс, який живив зростання економік країн, починаючи від XIX століття. Процеси цифровізації суспільства у XXI столітті спираються на обладнання, яке потребує енергії. За даними British Petroleum, у 2021 р. глобальний попит на первинну енергію зріс на 5,8%, а вуглецеві викиди від енергоспоживання зросли на 5,9%. Дефіцит викопного палива та відомі екологічні проблеми, пов'язані з вуглецевими викидами, допомагали посилювати увагу до відкриття альтернативних енергоджерел, серед яких найважливішими є такі відновлювані джерела, як сонячна та вітрова енергія [15]. Енергія, видобута з різних (традиційних і відновлюваних) джерел, генерується з боку пропозиції і доставляється споживачам з боку попиту. Менеджмент зростаючого попиту на енергію з боку пропозиції обмежується через реальні інфраструктурні та ресурсні умови мережі.

Смарт-контракти дозволяють вирішувати багато сучасних проблем енергетики України, зокрема відомі проблеми залучення малого і середнього бізнесу до енергогенерації для енергомереж. Сучасна енергетика має задовольняти критеріям ефективності, резильєнтності, керованості та іншим.

1. Горбачук В.М., Денис О.І. Застосування блокчейнових технологій для оподаткування. Тенденції розвитку публічних та корпоративних секторів економіки України в умовах макроекономічної нестабільності (29 січня 2020 р., Київ, Україна). Київ: НаУКМА, 2020. С. 24–26.
2. Saraji S., Borowczak M. A blockchain-based carbon credit ecosystem. White Paper. 2021. https://doi.org/10.48550/arXiv.2107.00185
3. Oprea S.V., Bâra A., Diaconita V. A motivational local trading framework with 2-round auctioning and settlement rules embedded in smart contracts for a small citizen energy community. Renewable Energy. 2022. 193, June. P. 225–239.
4. Ebrahimi M., Sheikhi A. A local integrated electricity-heat market design among multi smart energy hubs with renewable energy generation uncertainty. Electric Power Systems Research. 2023. 218, May. 109217.
5. Vieira G., Zhang J. Peer-to-peer energy trading in a microgrid leveraged by smart contracts. Renewable and Sustainable Energy Review. 2021. 143, June. 110900.
6. Richter L.L., Pollitt M.G. Which smart electricity service contracts will consumers accept? The demand for compensation in a platform market. Energy Economics. 2018. 72. P. 436–450.
7. Foroozandeh Z., Ramos S., Soares J., Vale Z., Dias M. Single contract power optimization: a novel business model for smart buildings using intelligent energy management. International Journal of Electrical Power & Energy Systems. 2022. 135, February. 107534.
8. Zhao S., Zhu S., Wu Z., Jaing B. Cooperative energy dispatch of smart building cluster based on smart contracts. International Journal of Electrical Power & Energy Systems. 2022. 138, June. 107896.
9. Горбачук В.М., Сирку А.А., Сулейманов С.-Б. Блокчейнові застосування у фінансах. Інфраструктура ринку. 2019. 35. С. 493–499.
10. Zhang T.-Y., Feng T.-T, Cui M.L. Smart contract design and process optimization of carbon trading based on blockchain: the case of China's electric power sector. Journal of Cleaner Production. 2023. 397, April 15. 136509.
11. Siddiqui S., Hameed S., Shah S.A., Khan A.K., Aneiba A. Smart contract-based security architecture for collaborative services in municipal smart cities. Journal of Systems Architecture. 2023. 135, February. 102802.
12. Chandra R., Radhakrishnan K.K., Panda S.K. Privacy protected product differentiation through smart contracts based on bilateral negotiations in peer-to-peer transactive energy markets. Sustainable Energy, Grids and Networks. 2023, June. 34. 100997.
13. Kirli D., Couraud B., Robu V., Salgado-Bravo M., Norbu S., Andoni M., Antonopoulos I., Negrete-Pincetic M., Flynn D., Kiprakis A. Smart contracts in energy systems: a systematic review of fundamental approaches and implementations. Renewable and Sustainable Energy Review. 2022. 158, April. 112013.
14. Горбачук В.М., Ляшко В.І., Сирку А.А. Питання децентралізованого консенсусу блокчейнів. Інфраструктура ринку. 2019. 34. С. 325–332.
15. Bao J., He D., Luo M., Choo K.-K.R. A survey of blockchain applications in the energy sector. IEEE Systems Journal. 2021. 15 (3). P. 3370–3381.

А.М. Давиденко, О.Ю. Беспалов., Л.В. Ковальчук

СТАТИСТИЧНИЙ КРИТЕРІЙ ПЕРЕВІРКИ НЕЗАЛЕЖНОСТІ БІТОВИХ ПОСЛІДОВНОСТЕЙ

У доповіді запропоновано, строго обґрунтований, статистичний критерій для перевірки попарної незалежності випадкових величин, реалізаціями яких є бітові послідовності. Також розроблено і чітко сформульовано відповідний алгоритм, який реалізує перевірку незалежності згідно до цього критерію. Отриманий інструмент є дуже актуальним при виконанні статистичної перевірки криптографічних якостей різних криптопримітивів, функціонування яких пов'язане з виробленням випадкових/псевдовипадкових послідовностей. До таких криптопримітивів належать не лише генератори випадкових/псевдовипадкових послідовностей, а й потокові алгоритми шифрування, комбіновані алгоритми шифрування (тобто блокові алгоритми у потокових режимах), тощо. Використання запропонованого критерію дозволить перевірити не тільки незалежність вихідних послідовностей, а й незалежність вихідних послідовностей від послідовностей внутрішніх станів, проміжних гам, вхідних даних. Зазначимо, що така незалежність є обов'язковою для того, щоб вихідну послідовність можна було вважати непередбачуваною.

На даний час відчувається суттєвий брак таких алгоритмів. У той час як велика увага приділяється статистичним якостям окремих послідовностей [1-4], питання про їх незалежність чомусь практично не розглядається. Єдиним доступним критерієм, який вдалося побудувати, базуючись на результатах [5], скористались, наприклад, для перевірки незалежності внутрішніх станів алгоритму «Кгір» [6].

Формалізація задачі.

Нехай $m, n \in \mathbf{N}$. Позначимо

$$X = \left\{ X^{(i)},\ i \in \overline{1,n} \right\} \tag{1}$$

множину послідовностей незалежних однаково розподілених випадкових величин, $X^{(i)} = \left(x_1^{(i)}, ..., x_m^{(i)} \right)$, де $x_k^{(i)} \in \{0, 1\}$, а також позначимо

$$a^{(i)} = Ex_k^{(i)} = P\left(x_k^{(i)} = 1 \right),\ \left(\sigma^{(i)} \right)^2 = Var\left(x_k^{(i)} \right). \tag{2}$$

Зокрема, послідовність $\left(x_1^{(i)}, ..., x_m^{(i)} \right)$ можна розглядати як реалізацію випадкової величини $X^{(i)}$.

Сформулюємо гіпотезу H_0 як "послідовності у множині (1) є попарно незалежними". Альтернативна гіпотеза H_1 є складною і формулюється як "гіпотеза H_0 не виконується".

Задача полягає у тому, щоб побудувати і обґрунтувати статистичний критерій, який буде розпізнавати гіпотезу H_0 із заданою імовірністю помилки першого роду α.

Позначення і допоміжні твердження.

У цьому розділі ми сформулюємо і доведемо ряд тверджень, потрібних для розв'язку задачі, сформульованої вище.

Розглянемо випадкові величини

$$r_k^{(i,j)} = \frac{\left(x_k^{(i)} - a^{(i)}\right)\cdot\left(x_k^{(j)} - a^{(j)}\right)}{\sigma^{(i)}\cdot\sigma^{(j)}}, \qquad i, j \in \overline{1,n},\ k \in \overline{1,m}. \quad (3)$$

Твердження 1.

Нехай послідовності $X^{(i)}$ та $X^{(i)}$ є незалежними. Тоді:

1) $E\left(r_k^{(i,j)}\right) = 0$, $Var\left(r_k^{(i,j)}\right) = 1$, $i, j \in \overline{1,n}$, $k \in \overline{1,m}$;

2) якщо при цьому виконується $a^{(i)} = \frac{1}{2}$, $i \in \overline{1,n}$, то $\left(r_k^{(i,i)}\right)^2 = 1$.

Для довільного $n \in N$, позначимо S_n групу всіх перестановок довжини n, а також позначимо $S_n^{(l)} \subset S_n$ підмножину перестановок, які мають рівно l нерухомих точок.

Твердження 2. Нехай $n \in N$, q – довільне додатне число, матриця $A = \left(a_{ij}\right)_{i,j=1}^{n}$ є квадратною матрицею, причому $a_{ii} = 1$, $i \in \{1,...,n\}$, а для інших елементів матриці виконується рівність $a_{ij} = a_{ji}$, $\forall i, j \in \{1,...,n\}$, та нерівність $\left|a_{ij}\right| \le q$, $\forall i, j \in \{1,...,n\}$, $i \ne j$.

Тоді справедлива наступна нерівність:

$$\left|\det A - 1 + \sum_{1\le i<j\le n} a_{ij}^{\,2}\right| \le e^{n^2 q} - 1 - n^2 q - \frac{n^3(n-1)}{2}\cdot q^2. \quad (4)$$

Наслідок 1.

Якщо в умовах Твердження 1 покласти $q = \frac{\delta}{n^2}$, для деякого $\delta \in (0,1)$, то з нерівності (4) отримаємо нерівність:

$$\left|\det A - 1 + \sum_{1\le i<j\le n} a_{ij}^{\,2}\right| \le e^{\delta} - 1 - \delta - \frac{\delta^2(n-1)}{2n},$$

що для достатньо великих n можна переписати як

$$\left|\det A - 1 + \sum_{1\le i<j\le n} a_{ij}^{\,2}\right| \le e^{\delta} - 1 - \delta - \frac{\delta^2}{2}.$$

Зокрема, при $\delta = 1$ маємо:

$$\left|\det A - 1 + \sum_{1\le i<j\le n} a_{ij}^{\,2}\right| \le e - 2.5. \qquad (5)$$

Позначимо $R^{(i,j)}$ величину, визначену за формулою:

$$R^{(i,j)} = \frac{1}{m}\sum_{k=1}^{m} r_k^{(i,j)}. \qquad (6)$$

Оскільки $R^{(i,j)}$ є середнім арифметичним незалежних випадкових величин з нульовим математичним сподіванням і одиничною дисперсією, то легко бачити, що

$$E\left(R^{(i,j)}\right) = 0 \text{ та } Var\left(R^{(i,j)}\right) = \frac{1}{m}. \qquad (7)$$

Зазначимо, що з нерівності $m > \frac{1}{\varepsilon \cdot q^2}$ випливає нерівність $m > \frac{\ln\frac{2}{\varepsilon}}{q^2}$, тому Твердження 4 дає більш точну нижню межу для значення m.

Побудова статистичного критерію перевірки гіпотези про незалежність послідовностей.

Побудуємо статистичний критерій перевірки незалежності послідовностей та відповідний алгоритм. Основну ідею, на які побудовано критерій, можна неформально описати так. Задамо деякий рівень значимості α (імовірність помилки I-го роду). Якщо послідовності (1) є попарно незалежними, то, вибравши їх довжини m достатньо великими (згідно до Тверджень 3 або 4), можемо побудувати таку матрицю $A = \left(R^{(ij)}\right)_{i,j=1}^{n}$, що її елементи будуть меншими за деяке значення q з імовірністю, не меншою за $1-\alpha$. Значення q при цьому обираємо так, щоб права частина (4) була достатньо малою – наприклад, $q = \frac{1}{n^2}$. Обчислюємо елементи матриці A та її визначник і перевіряємо виконання рівності (4). Згідно з вибором довжини послідовності, імовірність того, що нерівність (4) не буде виконуватись для попарно незалежних послідовностей, не перевищує α.

Алгоритм перевірки попарної незалежності послідовностей.

Вважається, що ми маємо доступ до джерел генерації послідовностей (1) і можемо отримувати з них послідовності достатньої довжини (потрібна довжина залежить від кількості n послідовностей та бажаного рівня значимості).

Слід зазначити, що наведений нижче алгоритм орієнтований на перевірку незалежності джерел, які генерують відповідні послідовності. Саме така задача є найбільш актуальною для практичних застосувань. Але, з певними модифікаціями, його можна використовувати і для перевірки незалежності заданих послідовностей.

Вхід: рівень значимості α ; кількість n перевіряємих послідовностей.

1. Обчислити $q = \frac{1}{n^2}$ та $m = \left\lceil \frac{\ln \frac{2}{\alpha}}{q^2} \right\rceil$.

2. Згенерувати (з відповідних джерел або одного джерела) n послідовностей $X^{(i)}$, $i \in \overline{1,n}$, довжини m.

Зауваження: генерувати послідовності не потрібно, якщо задача полягає в перевірці незалежності послідовностей з заданого набору.

3. Обчислити елементи матриці $A = \left(R^{(ij)} \right)_{i,j=1}^{n}$ за формулами (3) та (6).

4. Обчислити $d = \det A$.

5. Обчислити $t = \left| \det A - 1 + \sum_{1 \le i < j \le n} a_{ij}^{\,2} \right|$.

6. Якщо $t \le e - 2.5$, то гіпотеза H_0 приймається, в іншому випадку – відкидається.

Результати застосування Алгоритму.

Результати застосування алгоритму до незалежних послідовностей (отриманих з генератора, описаного у Додатку А ДСТУ 9041:2020, [7]) та залежних (лічильник та файл з розширенням avi) показали коректність роботи алгоритму.

1. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 1999. Rev. 1. – 131 p.
2. Marsaglia, G.: The Marsaglia random number CDROM including the DIEHARD battery of tests of randomness (1996), http://stat.fsu.edu/pub/diehard
3. Robert G. Brown, DieHarder: A Gnu Public License Random Number Tester, Version 3.31.2beta (2006) https://rurban.github.io/dieharder/manual/dieharder.pdf
4. Elena Almaraz Luengo, Luis Javier García Villalba, Recommendations on Statistical Randomness Test Batteries for Cryptographic Purposes, May 2021, ACM Computing Surveys 54(4):1-34, DOI: 10.1145/3447773
5. Anderson, T.W. (1958) An Introduction to Multivariate Statistical Analysis. John Wiley & Sons, New York. 500 p.
6. Krip: High-Speed Hardware-Oriented Stream Cipher Based on a Non-Autonomous Nonlinear Shift Register, Kovalchuk, L.V., Koriakov, I.V., Alekseychuk, A.N., *Cybernetics and Systems Analysis*, 2023, 59(1), pp. 16–26.
7. ДСТУ 9041:2020 Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=90523

А.М. Жорняк

ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН. СУЧАСНІ ВИКЛИКИ

Технологія блокчейн є перспективною інновацією, яка полягає у створенні децентралізованих, надійних та безпечних систем обліку та обміну інформацією. Її застосування може призвести до значних змін в організаційних структурах різних сфер суспільного життя, таких як, державне управління, судова система, економіка, логістика, охорона здоров'я, система голосування тощо [1].

Незважаючи на очевидні переваги, виникають серйозні правові виклики, пов'язані із законодавчим регулюванням технології блокчейн. Ці виклики охоплюють як національний так і міжнародний рівень, оскільки технологія блокчейн функціонує у глобальному просторі. Ефективне законодавче регулювання блокчейн є ключовим аспектом для її широкого застосування, з метою забезпечення добробуту суспільства, утримання соціальної стабільності, економічної цілісності та боротьби з кіберзлочинністю [2]. На міжнародному рівні відсутні універсальні, єдині законодавчі норми та стандарти щодо правового регулювання та широкого застосування технології блокчейн. Спроби законодавчого регулювання технології блокчейн створюють невизначеність, щодо можливих ризиків, пов'язаних із її використанням. Уряди країн ще не прийняли єдиний підхід, висловлюючи необхідність моніторингу та державного регулювання в процесі впровадження та застосування технології, виражаючи обережність щодо потенційних ризиків пов'язаних із використанням технології блокчейн. Ключові виклики у сфері законодавчого регулювання технології блокчейн включають в себе питання забезпечення безпеки, конфіденційності та захисту інформації, а також невизначеність стосовно правового статусу відповідних завантажених у мережу документів та смарт-контрактів [2].

Враховуючи динамічний характер розвитку цієї технології, сприяючи сучасним інноваціям та враховуючи їх вплив на суспільство та економіку, необхідна розробка міжнародних стандартів та узгодження принципів законодавчого регулювання технології блокчейн. Застосування цієї технології має значний потенціал для якісної трансформації різних галузей, включаючи зберігання інформації, реєстрацію транзакцій, проведення юридичних операцій тощо. Наразі вона перебуває на етапі досліджень, з великою кількістю нормативних питань, що вимагають вирішення перед широким впровадженням [1].

Для юридичного визнання технології блокчейн та її застосувань у якості безпечної та незмінної системи, яка забезпечує надійність інформації та унікальні функції ідентифікації, також необхідна відповідна правова база. Відсутність стандартизованого правового статусу перешкоджає застосування технології під час здійснення правових (юридичних) процедур [3].

Правова база, що регулює юридичну силу документів, збережених у мережі блокчейн, вимагає ретельної розробки та затвердження. Визнання блокчейну як унікального та достовірного джерела, вимагає не лише прийняття незмінності збереженої інформації, але і визнання юридичної сили документів, завантажених у мережу. На сьогоднішній день відповідне законодавство в цьому питанні також відсутнє, але його розробка стає необхідною складовою для забезпечення ефективності та визнання технології блокчейн [4].

У зв'язку з технологічною особливістю блокчейну, а саме - «незмінність блоків та захищеність від несанкціонованого доступу», виникає протиріччя з правом на видалення інформації, передбаченим європейським законодавством про захист персональних даних. Це право надає кожному громадянину Європи можливість вимагати видалення своїх персональних даних, які зберігаються в базах даних. Можливим рішенням для забезпечення відповідності правам на захист персональних даних за допомогою технології блокчейн може бути заміна права на «видалення» інформації, правом «заборонити використання» особистої інформації третіми особами [5].

При використанні технології блокчейн для визначення юридичного статусу фінансових інструментів, таких як акції та облігації, необхідно отримати визнання їх юридичної сили від державних регулюючих та наглядових органів. Одним із ключових фінансових інструментів, що може бути випущений у мережі блокчейн, є цифрові гроші та криптовалюта. Це може викликати значущі наслідки для фінансової системи та макроекономіки. Таким чином, необхідно розробити відповідні законодавчі та регуляторні рамки для визначення статусу та юридичної сили цифрових грошей а також забезпечити контроль з боку відповідних державних органів [6].

Законодавча база для смарт-контрактів також повинна включати загальні та міжнародні аспекти, а саме, територіальність та відповідальність. Урахування місцезнаходження розподіленого реєстру і різниць у законодавчих актах для сторін контракту є ключовим аспектом. Смарт-контракти включають обов'язки для сторін, розробників та сховища контракту, а також визначення відповідальності за розроблений контракт.

Також важливим питанням є регулювання використання блокчейн як реєстру для Інтернету речей. Створення загального реєстру для ідентифікації та управління підключеними пристроями також вимагає законодавчого визнання розподілених реєстрів. Усі питання, пов'язані з територіальністю, відповідальністю та застосуванням смарт-контрактів у мережі блокчейн, також впливають на функціонування Інтернету речей. Сучасні глобальні процеси та новітні ІТ-технології, зокрема технологія блокчейн, мають великий вплив на міжнародні відносини. У більшості країн відсутнє або тільки опрацьовується законодавство щодо регулювання, впровадження та широкого застосування цієї технології, що призводить до ризиків які можуть спричинити кіберзлочинці.

Необхідність законодавчого регулювання при широкому використання технології блокчейн є вкрай важливою складовою, оскільки ця технологія широко використовується у всьому світі та зазнає постійного розвитку. Метою держав має стати впровадження заходів для розробки та впровадження технології блокчейн у межах діючого законодавства, офіційного визнання криптовалют та електронних грошей, а також регулювання відносин, пов'язаних з їх володінням, зберіганням та використанням [7].

Політика різних країн щодо організаційно-правового регулювання, впровадження та застосування технології блокчейн на міжнародному рівні виявляється нерівномірною [5]. У деяких країнах спостерігаються певні кроки у цьому напрямку, проте глобально ці процеси розгортаються досить повільно.

Розглядаючи питання необхідності модернізації законодавства у галузі технології блокчейн, рекомендується враховувати наступні аспекти: створити єдино визнані визначення та терміни, такі як «блокчейн», «криптовалюта», «смарт-контракт»; інституціоналізувати управління через централізовані регулюючі органи надавши їм відповідні повноваження; визначити стандарти кібербезпеки та розробити заходи для протидії кіберзлочинності; створити систему оподаткування для криптовалют та криптоактивів; забезпечити сприятливі умови для розвитку технології блокчейн, включаючи підтримку стартапів; розвивати міжнародне партнерство та стандарти регулювання на міжнародному рівні; регулювати фінансові установи, які використовують технологію блокчейн для мінімізації ризиків та фінансової стабільності; залучати експертів, бізнес, науковців та громадськість для розробки рекомендацій щодо поліпшення законодавства у галузі регулювання технології блокчейн; стандартизувати технічні аспекти для сумісності між різними системами; розробити та впровадити державні програми для фінансування досліджень та підготовки відповідних кваліфікованих кадрів. Ці заходи сприятимуть інноваціям і інтеграції блокчейн у різні галузі, розширюючи можливості для суспільства, забезпечуючи безпеку та захист інтересів користувачів [8].

Розробка законодавства для регулювання відносин щодо використання децентралізованих мереж вимагають інноваційних підходів, спрямованих на загальний добробут суспільства, збереження соціальної стабільності, економічної стійкості, боротьби з кіберзлочинністю та захисту прав користувачів [3]. Цей напрям є динамічним та знаходиться на стадії розвитку. Досвід провідних країн світу важливий для визначення оптимальної моделі регулювання. Існуючі світові підходи розрізняються від суворого контролю до ліберальних режимів. Різні країни обирають стратегії від заборони до створення спеціальних фінансових зон. В світовій практиці застосовуються різні методи, включаючи ліцензування, оподаткування та саморегулювання. Кожен підхід відображає потреби та пріоритети конкретної країни [5].

Стрімкий розвиток технології блокчейн випереджає створення відповідного законодавства, що ускладнює процес правового регулювання

яке відіграє ключову роль у забезпеченні її впровадження, а також соціально-економічних інтересів користувачів, фінансовій стабільності, сприяючи боротьбі з кіберзлочинністю [7]. Розробка та впровадження відповідного законодавства, створення єдиної методології законодавчого регулювання, вимагають ефективної міжнародної співпраці, узгоджених рішень та участі всіх зацікавлених сторін, включаючи державні органи, бізнес та громадськість. Здійснення прозорого, зрозумілого та етичного регулювання повинно враховувати практичні аспекти використання технології блокчейн у різних сферах її застосування.

1. Даньшина Ю. В., Брітченко І. Г. Переваги, можливості та недоліки технології блокчейн // Фінансово-кредитний механізм активізації інвестиційного процесу: збірник матеріалів III Міжнародної науково-во-практичної конференції (м. Київ, 10 листопада 2017 р.). Київ : КНЕУ, 2017. С. 106–109.
2. Чекаловська Г. З., Лось А. А. Сучасні тенденції розвитку blockchain технологій в Україні. Регіональна економіка та управління. 2019. № 4. Ч. 2. С. 153–157.
3. Літошенко А. В. Технологія Blockchain: переваги та неочевидні можливості використання у різних галузях» [Електронний ресурс], - Режим доступу: http://www.economy.in.ua/pdf/8_2017/20.pdf (дата звернення 12.12.23).
4. Пантєлєєва Н. М. Інноваційна технологія блокчейн у системі управління державними фінансами. Науковий вісник Ужгородського університету. Серія «Економіка». 2018. Вип. 1. С. 363–369. DOI: https://doi.org/10.24144/2409-6857.2018.1(51) (дата звернення: 12.12.2022).
5. Cooperation on a European Blockchain Partnership [Електронний ресурс]: (Declaration 2018), - Режим доступу: https://www.scribd.com/document/398159396/2018DeclarationonEuropeanPartnershiponBlockchainpdf-pdf (дата звернення: 08.05.2022).
6. Бондаренко О. В. Запровадження технології блокчейн у державному секторі [Електронний ресурс]: (Протокол), - Режим доступу: https://bit.ly/3lFNCET (дата звернення: 12.12.2022).
7. Гурова А., Кірпачова М. Правові засади застосування блокчейну в космічній діяльності: особливості регулювання технології на національному, регіональному та міжнародному рівнях. Підприємництво, господарство і право. 2021. № 1. С. 265-275.
8. Бородіна О.А., Ляшенко В.І. Повоєнне відновлення економіки: світовий досвід та спроба його адаптації для України. Вісник економічної науки України. 2022. 1 (42). С. 121-134.

М.В. Кацюба, Г.В. Неласа

ВИКОРИСТАННЯ НЕІНТЕРАКТИВНОГО ПРОТОКОЛУ ДОКАЗУ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ В СХЕМАХ АВТЕНТИФІКАЦІЇ

На сьогоднішній день існує багато способів автентифікації користувачів[1]. Традиційним вважається парольний спосіб автентифікації, тобто вхід у систему здійснюється за допомогою паролю. Системи, що використовують даний спосіб автентифікації найпростіше всього реалізувати, але при цьому безпека даних у більшій мірі залежить від самого користувача, що придумав пароль. Крім того, бази даних, що зберігають хешовані паролі, часто зламують, і, як наслідок, виникають витоки баз паролів. Також існують біометричні та апаратні методи автентифікації. Біометрична автентифікація здійснюється на основі фізіологічних та поведінкових характеристик людини (відбитки пальців, райдужна оболонка ока, геометрія руки й обличчя, рукописний почерк, клавіатурний почерк, розпізнавання голосу тощо). Апаратна автентифікація здійснюється за допомогою унікальних предметів (магнітні карти, смарт-карти, USB-токени тощо) [2]. Біометрична й апаратна автентифікація забезпечують більш надійний захист, ніж парольна автентифікація, проте вони вимагають додаткового апаратного й програмного забезпечення. Досить поширеним є багатофакторна автентифікація, яка здійснюється в результаті комбінації двох або більше різних однофакторних методів (наприклад, пароль і відбиток пальця, пароль і SMS з одноразовим кодом підтвердження тощо). Даний вид автентифікації забезпечує надійний захист, але його основним недоліком є складність використання непідготовленими користувачами.

Одним із сучасних методів автентифікації є автентифікація з використанням систем доказів з нульовим розголошенням. Доказ із нульовим розголошенням — це криптографічний протокол, який дозволяє одній стороні (тому, хто доводить) переконати іншу сторону (верифікатора) у правдивості твердження, не розкриваючи жодної додаткової інформації про себе (наприклад, не надавати жодних подробиць про те, що саме було доведено чи звідки взята ця інформація).[3]

Приклади проєктів, які використовують докази з нульовим розголошенням в автентифікаційних системах:

1. ProtonMail. Використовує протокол SRP (Secure Remote Password) – протокол парольної автентифікації, який дозволяє користувачеві взагалі не надсилати пароль на сервер. Це приклад доказу з нульовим розголошенням: користувач доводить серверу, що знає пароль, не розкриваючи самого пароля. На етапі реєстрації клієнтська програма (браузер) обчислює та відправляє на сервер так званий верифікатор. При генерації верифікатора використовується пароль, але пароль ніколи не потрапляє на сервер. Відновити пароль за допомогою верифікатора неможливо.[4] Цей протокол є

прикладом інтерактивної системи доказу з нульовим розголошенням, тобто користувач і сервер знаходяться у постійній взаємодії.

2. Iden3. Використовує принцип неінтерактивної взаємодії, тобто після запиту автентифікації від сервера користувач самостійно генерує доказ і один раз відправляє його серверу на перевірку. Загальна схема автентифікації зображена на рис.1 [5]. В автентифікації Iden3 використовуються докази Groth16 [6].

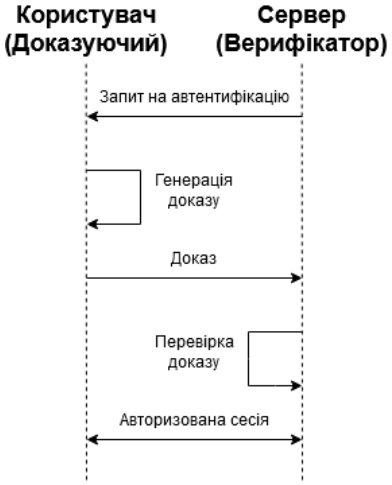


Рисунок 1 - Схема автентифікації Iden3

Метою роботи є реалізація схеми автентифікації від iden3, яка використовує сучасний неінтерактивний протокол доказу з нульовим розголошенням.

У якості неінтерактивного протоколу з нульовим розголошенням було обрано сучасний протокол Plonky2 [7]. Він є рекурсивним протоколом, тобто він розбиває доказ на окремі докази, які обчислюються паралельно, і потім об'єднуються в один доказ. Також цей протокол використовує основне поле вигляду $p = 2^{64} - 2^{32} + 1$, яке дозволяє оптимізувати швидкість обчислень з боку апаратного забезпечення. За рахунок цього Plonky2 є швидким протоколом, який можна використовувати у системах, де швидкодія є одним з основних критеріїв.

У якості програмування була вибрана мова програмування Rust. Ця мова має строгу типізацію і сфокусована на безпечній роботі з пам'яттю. Автоматичне керування пам'яттю позбавляє розробника необхідності маніпулювання вказівниками й захищає від проблем, що виникають через низькорівневу роботу з пам'яттю, таких як звернення до ділянки пам'яті після її звільнення, розіменовування нульових вказівників, вихід за межі буфера тощо.

Для Rust існує окрема бібліотека plonky2, яка реалізовує внутрішній механізм роботи протоколу Plonky2 і дозволяє зручно використовувати і вбудовувати цей протокол у проєкти.

У даній роботі було досліджено можливість використання систем доказів з нульовим розголошенням для побудови систем автентифікації користувачів. Розглянуто готові рішення автентифікації, що використовують системи доказів з нульовим розголошенням. На даний момент активно розробляється практична реалізація даної системи автентифікації на мові програмування Rust.

1. Клопотовський Д., Писаренко Л. Класифікація механізмів аутентифікації користувачів і їх огляд. Перспективні напрямки сучасної електроніки : Матеріали науково-практ. конф., 06.04.2017 р.
2. Литвин В., Мандрона М. Аналіз методів автентифікації в інформаційних системах.
3. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems. SIAM journal on computing. 1989. Т. 18, № 1. С. 186–208.
4. Butler B. Improved authentication for email encryption and security | Proton. Proton. URL: https://proton.me/blog/encrypted-email-authentication.
5. Login protocol - iden3 documentation. Iden3 Documentation. URL: https://docs.iden3.io/protocol/zklogin/.
6. Groth J. On the Size of Pairing-based Non-interactive Arguments. 2016.
7. GitHub - 0xPolygonZero/plonky2. GitHub. URL: https://github.com/0xPolygonZero/plonky2.

Л.В. Ковальчук, А.А. Вихло

ОБЧИСЛЕННЯ ІМОВІРНОСТІ УСПІХУ АТАК ВИПЕРЕДЖЕННЯ

Атака випередження – атака на смарт контракти, сутність якої полягає в зміні порядку транзакцій в блоці за допомогою підвищення комісії транзакцій зловмисника. Метою такої атаки є отримання неправомірної вигоди за рахунок отримання кращих умов при зміні порядку включення транзакцій в блок [1].

Далі розглянемо два типи такої атаки - атака заміщення і атака вставки [2]. Нижче ми коротко опишемо сутність кожної з атак та оцінимо імовірність успіху при заданих вхідних даних.

Атака типу заміщення полягає в отриманні неправомірної вигоди за рахунок випередження іншого учасника аукціону. Часто виконується за допомогою створення дублюючої транзакції зловмисником і підвищенням її комісії значно вище оригінальної. До такої атаки особливо вразливими є аукціони [3], так як випередивши виграшну ставку, можна виграти лот іншого учасника.

Атака типу вставки полягає у створенні двох транзакцій з подальшим включенням їх в блок таким чином, щоб оригінальна транзакція потрапила в блок між транзакціями зловмисника . Вигода часто досягається за допомогою зміни умов купівлі та продажу активів, змінюючи його попит. Тобто купівлі за низького попиту, і продажу за високого, який було штучно створено [4].

Для формулювання основних результатів стосовно обчислення імовірності успіху атаки, необхідно навести наступні леми з теорії імовірності.

Лема 1.

Припустимо, що ξ_1 та ξ_2 випадкові величини з експоненційним розподілом та параметрами λ_1 та λ_2:

$$F_i(t) = P(\xi_i \le t) = 1 - e^{-\lambda_i \cdot t}, \quad i \in \{1,2\}. \tag{1}$$

Тоді для будь-якого $\Delta > 0$ справедливо:

$$P(\xi_2 < \xi_1 + \Delta) = 1 - e^{-\lambda_2 \cdot \Delta} \cdot \frac{\lambda_1}{\lambda_1 + \lambda_2}. \tag{2}$$

Наслідок 1.

Якщо $\Delta = 0$, то лема 1 набуває наступну форму:

$$P(\xi_2 < \xi_1) = \frac{\lambda_2}{\lambda_1 + \lambda_2}. \tag{4}$$

Теорема 1 (імовірність успіху атаки заміщення).

Позначимо час обробки транзакції з комісією τ як випадкову величину T_τ. Припустимо, що T_τ має експоненційний розподіл з параметром $\lambda = \lambda(\tau)$. Позначимо Δ – час створення дублюючої транзакції зловмисником, τ_1 – комісія оригінальної транзакції, τ_2 – комісія дублюючої транзакції.

Тоді формула обчислення імовірності успіху атаки типу заміщення має наступний вигляд:

$$P_{dis}(\tau_1, \tau_2, \Delta) = e^{-\lambda(\tau_1)\cdot\Delta} \cdot \frac{\lambda(\tau_2)}{\lambda(\tau_1)+\lambda(\tau_2)}. \quad (5)$$

Наслідок 2.

Формулу імовірності успіху в такому разі можна обмежити зверху і ця оцінка не залежить від комісії транзакції зловмисника:

$$P_{dis}(\tau_1, \tau_2, \Delta) < e^{-\lambda(\tau_1)\cdot\Delta}. \quad (6)$$

Теорема 2 (імовірність успіху атаки вставки).

Позначимо час обробки транзакції з комісією τ як випадкову величину T_τ. Припустимо, що T_τ має експоненційний розподіл з параметром $\lambda = \lambda(\tau)$. Позначимо Δ – час створення двох транзакцій зловмисником, після аналізу оригінальної транзакції, τ_1 – комісія оригінальної транзакції, τ_2 – комісія транзакції зловмисника, τ_3 – комісія другої транзакції зловмисника.

Тоді формула обчислення імовірності успіху атаки типу вставки має наступний вигляд:

$$P_{ins}(\tau_1, \tau_2, \tau_3, \Delta) = e^{-\lambda(\tau_1)\cdot\Delta} \cdot \frac{\lambda(\tau_2)}{\lambda(\tau_1)+\lambda(\tau_2)} \cdot \left(1 - e^{-\lambda(\tau_1)\cdot\Delta} \cdot \frac{\lambda(\tau_3)}{\lambda(\tau_1)+\lambda(\tau_3)}\right) \quad (7)$$

Наслідок 3.

Відповідно до теореми 2, імовірність успіху атаки вставки можна обмежити зверху наступним чином:

$$P_{ins}(\tau_1, \tau_2, \tau_3, \Delta) \leq 1 - e^{-\lambda(\tau_1)\cdot\Delta} \cdot \frac{\lambda(\tau_3)}{\lambda(\tau_1)+\lambda(\tau_3)}. \quad (8)$$

Висновки

Основними результатами цієї роботи є отримання явних формули для обчислення імовірностей успіху атак вставки та заміщення, що є частковими випадками атаки випередження. Ці формули показують залежність такої імовірності від розміру комісій транзакцій та часу, необхідного на створення транзакцій зловмисника, що допомагає аналізувати доцільність атаки та оцінювати рівень загрози.

Основним вектором подальшого дослідження є аналіз залежності середнього часу обробки та комісії транзакції для різних блокчейн мереж. Результати цього дослідження є суттєвими для більш точної оцінки імовірності успіху атак випередження.

1. Gandal, N., Hamrick, JT, Moore, T., Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. Journal of Monetary Economics. https://doi.org/10.1016/j.jmoneco.2017.12.004
2. Li, J., Yuan, Y., Wang, S., Wang, F. (2018). Transaction Queuing Game in Bitcoin BlockChain. IEEE Intelligent Vehicles Symposium (IV). https://doi.org/10.1109/IVS.2018.8500403
3. Paulavičius, R., Grigaitis, S., Filatovas, E., (2021). A Systematic Review and Empirical Analysis of Blockchain Simulators. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3063324
4. Capponi, A., Jia, R. (2021). The Adoption of Blockchain-based Decentralized Exchanges. arXiv. https://doi.org/10.48550/arXiv.2103.08842

М.С. Кондратенко

ПЕРЕВАГИ, НЕДОЛІКИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ НА РИНКУ ЕНЕРГЕТИКИ УКРАЇНИ

Розвиток цифрових технологій кардинально змінює основи та інструменти, що лежать в основі функціонування фінансових ринків у розвинутих країнах. Однією з новаторських технологій, яка визначила вектор подальших змін у багатьох сферах, стала блокчейн-технологія. Завдяки появі та швидкому розвитку блокчейн-платформ з'явився новий тип договорів — смарт-контракти або «розумні угоди». Смарт-контракт представляє собою формальну угоду, створену у вигляді комп'ютерного коду, яка може бути укладена, змінена або припинена лише через певну комп'ютерну програму. Така угода виконується автоматично і безперервно, без необхідності залучення третьої довіреної сторони, та здатна функціонувати навіть в умовах повної недовіри між учасниками.

Особливості роботи смарт-контрактів дозволяють підвищити рівень довіри між учасниками контракту. Прозорість, незмінність і відстежуваність транзакцій у блокчейні створюють більш сприятливе середовище для бізнесу, ніж будь-яка інша сучасна технологія обліку енергоресурсів, де існують корупція та людський фактор. Смарт-контракти можуть застосовуватися в багатьох сферах – від розробки альтернативних валют до управління транзакціями на енергетичних ринках.

Розумні контракти можуть змінити спосіб ведення бізнесу. Вони внесуть радикальні зміни шляхом прискорення транзакцій, скорочення бюрократії та підвищення загальної сукупної ефективності. Багато галузей, таких як музика, мистецтво, фінанси, роздрібна торгівля, нерухомість, телекомунікації та ланцюги поставок, можуть отримати значну користь від використання смарт-контрактів. Однак справжній потенціал смарт-контрактів доки не доступний через обмеження інфраструктури: вона лише зароджується. [1]

Розглянемо детальніше переваги застосування «розумних угод» на ринку купівлі-продажу електроенергії. Зокрема, можна виділити наступні:

1. Швидкі розрахунки, проводяться негайно після факту споживання електроенергії.
2. Зручний вибір параметрів тарифікації та управління трафіком.
3. Відсутність проблем з боржниками завдяки автоматизованій системі розрахунків.
4. Відмова від посередників, що призводить до зниження ціни на електроенергію на 5-10%.

Такі смарт-контракти ініціюються однією із сторін (споживачем, мережею або генеруючою компанією) і укладаються після узгодження всіх деталей. [2]

До недоліків та ризиків використання смарт-контрактів можна віднести їх неоднозначний юридичний статус. Причина полягає не лише в тому, що

блокчейн знаходиться в «сірій правовій зоні» для більшості країн, але й тому, що смарт-контракти не відповідають чинній правовій базі. Наприклад, часто для укладання контрактів необхідно, щоб обидві сторони були належним чином ідентифіковані та старші за 18 років. Псевдоанонімність, що забезпечується блокчейн технологією, у поєднанні з відсутністю посередників, не дозволяє належним чином виконувати ці вимоги. Хоча існують потенційні шляхи вирішення цього питання, юридична сила смарт-контрактів є реальною проблемою, особливо коли йдеться про розподілені мережі, в яких відсутнє будь-яке централізоване регулювання. [3]

Окрім цього, існують також наступні перешкоди на шляху до повноцінного впровадження «розумних угод» на енергетичному ринку України:

- **Технічна складність та ризики.** Висока складність створення та впровадження смарт-контрактів потребує спеціалізованих знань і навичок.Можливі помилки в коді контракту можуть призвести до небажаних наслідків, таких як неправильне виконання умов контракту.
- **Інфраструктурні обмеження.** Недостатньо розвинена інфраструктура блокчейн в Україні може стати перешкодою для широкого впровадження смарт-контрактів. Витрати на впровадження та підтримку блокчейн-інфраструктури будуть досить значними впродовж всього процесу.
- **Обмежена адаптивність.** Традиційні учасники енергетичного ринку можуть бути неготовими до переходу на нові технології через консервативність і звиклість до існуючих систем.

Враховуючи ці недоліки, впровадження смарт-контрактів на енергетичному ринку України потребує ретельного планування, врахування правових аспектів, розвитку технічної інфраструктури та підвищення обізнаності учасників ринку щодо нових технологій.

1. Смарт контракт: розумний код рулить. (2020). Na chasi. Crypto. https://nachasi.com/crypto/2020/12/08/smart-kontrakt/
2. Л.В. Ковальчук, М.С. Кондратенко (2023). Аналіз юридичного статусу смарт-контрактів та проблем, які виникають при узгодженні їх з законодавством України. Міжнародна науково-практична конференція «Живучість та резильєнтність – 2023». Збірник матеріалів конференції, 18–20. https://ipme.kiev.ua/wp-content/uploads/2023/11/Матеріали_конференції_Survivability_and_Resilience-2023-4.pdf
3. М.С. Кондратенко (2023). Узгодження математичних та юридичних аспектів при використанні смарт-контрактів. Наукові праці ДонНТУ Серія “Інформатика, кібернетика та обчислювальна техніка” №2 (37), 2023. Збірник матеріалів конференції, 54–66. https://iktv.donntu.edu.ua/wp-content/uploads/2024/03/06_kondratenko.pdf

Н.В. Кучинська

ОСОБЛИВОСТІ ПРОВАДЖЕННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ТОРГІВЛІ ЕНЕРГІЄЮ ЕЛЕКТРОТРАНСПОРТУ

Сучасний розвиток технологій поступово прямує до того, що блокчейн технології надають широкий спектр можливостей для розв'язання найактуальніших завдань в галузі викопної та відновлюваної енергії. Одним з провідних проектів щодо перспективних досліджень існуючих, нових та потенційних застосунків на основі технології блокчейн для промислових/нефінансових секторів є #Blockchain4EU[1]. Проект поєднав наукові та технологічні дослідження, результатом яких стало проектування та створення п'яти прототипів, спрямованих на фізичну демонстрацію того, як технологія блокчейн може бути застосована у п'яти конкретних секторах: енергетика, транспорт і логістика, творчі індустрії, передове виробництво та охорона здоров'я. Проведені дослідження є однозначним сигналом про низку важливих проблем, пов'язаних із технологією блокчейн. Одне з можливих застосувань стосується використання смарт-контрактів в блокчейн для автоматичного керування потоками попиту та пропозиції майже в реальному часі та для оптимального використання наявної енергії. Проект надає особливої увагу наступним ідеями впровадження технології:

- блокчейн все ще є експериментальною технологією на ранній стадії формування;
- важливими є вибір типу мережі блокчейн (публічний, приватний або гібридний) та питання масштабування, споживання енергії, безпеки, конфіденційності та захисту даних;
- розроблені технічні рішення, зокрема протоколи, повинні бути сумісними для різних продуктів та послуг.

Серед інших галузей проект також передбачає застосування технології блокчейн в енергетичному секторі, коли мова йде, наприклад, про розумну енергосистему, керування електромережами та мікромережами, однорангову торгівлю енергією, мікротранзакції чи платежі, торгівлею викидами вуглецю, моніторинг виробництва та споживання енергії, закупівлю відновлюваної енергії або зарядку електромобілів.

У Європі на транспортний сектор припадає близько 23% [2] викидів парникових газів, і здебільшого залежить від нафти. Дії щодо зміни клімату набирають обертів по всій Європі, підтримуючи масове поширення електротранспорту з метою досягнення до 2050 року цільових показників вуглецевої нейтральності, визначених Європейською Комісією. Тим не менш, збільшення кількості електротранспорту та електромобілів зокрема ставить перед приватними користувачами, населеними пунктами та енергетичною галуззю загалом певні завдання, пов'язані з умовами масового розгортання інфраструктури, зручної для використання електромобілів. Означені проблеми призвели до створення проекту EV4EU.

Доповідь містить аналізу проблем та можливих рішень щодо моделі централізованого управління енергією електромобілів, серед яких можна виділити складності масштабування, відсутність анонімності та конфіденційності. Зі збільшенням кількості учасників і обсягу транзакцій централізована мережа серйозно обмежує операційну ефективність системи, яка не може задовольнити вимоги масових масштабів транзакцій і обробки даних, також безпека даних не може бути гарантована. Тому надзвичайно важливо розробити прозору, безпечну та ефективну модель і метод торгівлі [3]. Інтеграція технології блокчейн в управління енергією електромобілів не тільки можлива, але й необхідна, оскільки може ефективно вирішити проблеми конфіденційності та безпеки в централізованому управлінні енергією електромобілів, а також може забезпечити безпечну та ефективну гарантію оптимального планування електромобілів.

У більшості досліджень впровадження блокчейн для торгівлі енергією електромобілів в основному використовується традиційна блокчейн-архітектура Bitcoin або Ethereum. Проте, оскільки пропускна здатність транзакцій в цих мережах обмежена, а дані транзакцій прозорі для всіх вузлів у загальнодоступному проекті блокчейну, досліджується також можливість вибору іншої архітектури мережі, яка б відповідала вимогам щодо продуктивності такої торгівлі. Деякі дослідники пропонують використовувати блокчейн консорціуму, який є слабко централізованим, щоб підвищити ефективність і безпеку торгівлі енергією.

Розподілене управління, оптимізація торгівлі енергією електричних транспортних засобів через блокчейн може не тільки задовольнити вимоги щодо конфіденційності користувачів, але й вимоги, пов’язані з автономною роботою суб’єктів. Процес торгівлі енергією на основі блокчейн можна розділити на фази, такі як розповсюдження інформації, узгодження, розрахунок і зберігання. Базуючись на механізмі однорангової торгівлі електроенергією, ціну електроенергії та кількість електроенергії, що продається між електромобілями, можливо формувати за допомогою смарт-контрактів у блокчейні з використанням механізмів аукціону. Також торгові платформи на основі блокчейну повинні надавати можливості динамічного ціноутворення.

1. *#Blockchain4EU: Blockchain for Industrial Transformations.* JRC Publications Repository https://publications.jrc.ec.europa.eu/repository/handle/JRC111095
2. *EV4EU.* Electric vehicles management for carbon neutrality in Europe. https://ev4eu.eu/
3. Ma, W., Hu, J., Yao, L., Fu, Z., Morais, H., Marinelli, M.: New technologies for optimal scheduling of electric vehicles in renewable energy-oriented power systems: A review of deep learning, deep reinforcement learning and blockchain technology. *Energy Convers. Econ*. 3, 345–359 (2022). https://doi.org/10.1049/enc2.12071

Л.В. Ковальчук, Г.В. Неласа, Н.В. Кучинська, О.В. Неласий

АНАЛІЗ ДОСВІДУ ВИКОРИСТАННЯ ДЕЦЕНТРАЛІЗОВАНОГО ЗАСТОСУНКУ SUNCONTRACT NFT

З оляду на сучасний стан енергетичної системи України, наближення ери децентралізованої енергетики, про яку сьогодні так багато говорять в світі, є не розкішшю, а нагальною потребою. В доповіді представлено аналіз досвіду роботи компанії «SunContract» на ринку зеленої енергії. [1]. За твердженням розробників, SunContract — це платформа, яка безпосередньо об'єднує виробників і споживачів електроенергії в пул (SunContract Energy Pool) для торгівлі на основі смарт-контрактів, що є новим підходом до однорангової торгівлі електроенергією[2]. SunContract здатний забезпечувати велику кількість домогосподарств і підприємств відновлюваною енергією, сприяючи зменшенню залежності від викопного палива. Проект впровадженно в Словенії та планується до експортування та адаптації для інших країн (зокрема, вже розгорнуто в Хорватії). Учасником SunContract Energy Pool може стати будь-хто (потенційний клієнт-споживач, або поставщик електроенергії), але для того, щоб отримати можливість торгівлі, потрібно придбати токени SunContract (SNC). Інформація щодо транзакцій та код смарт-контракту є доступними за посиланням [3].

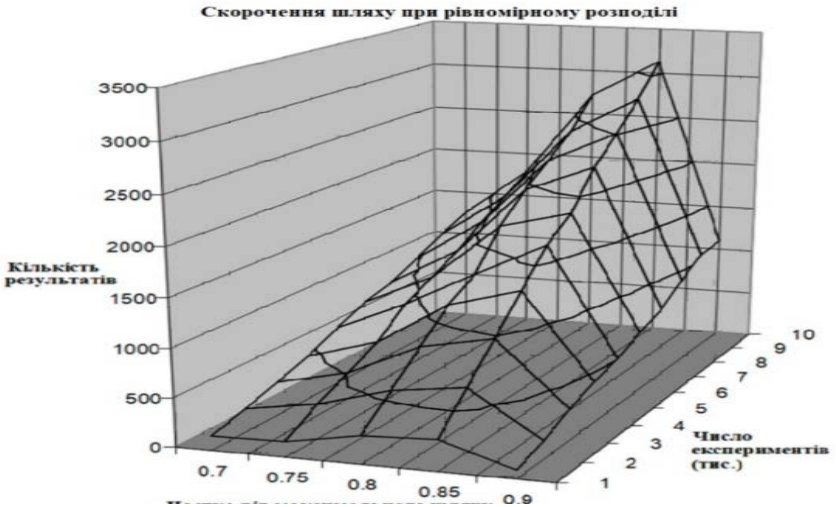
Новим напрямком розвитку компанії з грудня 2023 року є використання невзаємозамінних SunContract NFT токенів (non-fungible token). Невзаємозамінний NFT токен — це криптографічний токен, який не можна обміняти на інший. Власник такого NFT-токену володіє цифровим активом, що представляє справжню сонячну панель, яка виробляє електроенергію відповідно до умов використання NFT-ринку. Це дозволяє йому як використовувати вироблену енергію на свої потреби так і отримувати дохід. Ціни на електроенергію змінюються залежно від спотової ціни та цін на торгівлю електроенергією P2P під час транзакції відповідно до умов і положень ринку NFT. Користувачі, які мають дійсний контракт на споживання електроенергії із SunContract, мають доступ до платформи торгівлі електроенергією P2P, де можуть укладати приватні угоди на використання електроенергії, виробленої сонячними панелями, що лежать в основі їх NFT [4].

1. Suncontract is a blockchain-based P2P energy trading platform https://suncontract.org/
2. Decentralized Energy Market. Suncontract whitepaper. An energy trading platform that utilises blockchain technology to create a new disruptive model for buying and selling electricity. April 2017. https://suncontract.org/wp-content/uploads/2020/12/whitepaper.pdf
3. Etherscan Token SunContract (SNC) https://etherscan.io/token/0xF4134146AF2d511Dd5EA8cDB1C4AC88C57D60404/#code
4. Reshape the future of clean energy with SunContract NFT's https://nft.suncontract.org/

О.А. Сулима, О.О. Висоцка, С.О. Скворцов

ВИКОРИСТАННЯ ДВОРІВНЕВОЇ МОДЕЛІ ДОСТУПУ

Використання дворівневої моделі доступу до даних дозволяє створити програмне забезпечення, яке за певних умов може отримати доступ до інформації більш високого рівня доступу, не розголошуючи її змісту. Розглянемо прикладну задачу, не розкриваючи повністю предметну область інтерпретації, а обмежившись лише критичними умовами її реалізації. Задано три суміжні області A, B, C. Причому області A і C не мають спільних кордонів і шлях з A в C пролягає через B. У області B розташовано деякі об'єкти, інформація про які є конфіденційною. Нам необхідно прокласти шлях суб'єкту з області A в область C. При цьому суб'єкт не повинен наближатися до об'єкту на відстань D для попередження розголошення конфіденційної інформації про об'єкт з області B. Класична модель доступу вирішує цю проблему за рахунок обходу області B межею. Використовуючи дворівневу модель доступу до даних, можна побудувати критерій нерозголошення конфіденційної інформації. Наприклад, дозволити рух об'єкта в області B та аналізуючи траєкторію його руху, з метою не допущення його попадання в деяку область контакту об'єктів із області B. За рахунок цього буде відбуватися скорочення проходження шляху об'єкта. Проведемо серії експериментів: генеруючи в області B чотири об'єкти, випадковим чином дотримуючись рівномірного розподілу (завдання контролю об'єкта, забороненої території і території обмеженого доступу), для об'єкта з області A будується гарантований обхідний маршрут і будується маршрут проходження через область B з деякою точністю H. Критерієм нерозголошення встановимо не допущення наближення об'єкта з області A до об'єктів з області B на відстань D. Алгоритм пошуку шляху у таких умовах працює не отримуючи інформації про розташування об’єктів області B, що відповідає нашим вимогам з конфіденційності. Результатом експерименту буде розрахунок довжини скороченого шляху у частках від максимального (обхідного) шляху.



На рисунку приведено графічні результати проведених експериментів при зростанні їх числа. Аналізуючи отриману поверхню видно, що із збільшенням кількості проведених експериментів форма кривої наближається до класичної для нормального розподілу. Математичне сподівання частки шляху становить 0,8113, тобто середній виграш від застосування дворівневої моделі при 10000 експериментах становить майже 19% від максимального шляху.

В.Є. Чевардін, І.В. Лаврик, О.О. Прийма

МЕТОД ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ІЗОГЕНІЙ ЕЛІПТИЧНОЇ КРИВОЇ

Ізогенія еліптичної кривої (φ) в математичному сенсі – це гомоморфізм еліптичної кривої (ЕК), що зберігає групову структуру. Це означає, що арифметичні операції на кривій можуть бути відображені через ізогенію. Тобто, якщо P і Q є точками на кривій E, то:

$$\varphi(P + Q) = \varphi(P) + \varphi(Q).$$

Використовуючи ізогенні перетворення, можна створити надійні та важко передбачувані механізми для генерації псевдовипадкових послідовностей (ПВП). Схема генерації ПВП з використанням ізогеній базується на таких принципах:

- вибір початкової кривої та точки. Визначення еліптичної кривої E і базової точки P. Ця точка використовується як вихідний елемент для генерації ізогеній. Важливо, щоб точка P мала велике значення $ord(P)$, що сприяє криптографічній стійкості;
- генерація ізогеній. Розвиваючи послідовність ізогеній, можна трансформувати криву E у нову криву E'. Кожна ізогенія визначається ядром, згенерованим з точки P або її кратних. Це перетворення допомагає змінити властивості кривої, зберігаючи при цьому її групову структуру;
- перехід між кривими. Застосування послідовності ізогеній дозволяє перейти від кривої E до кривої E', і далі до інших кривих. На кожному етапі можна вибрати нові точки, що генеруються на базі $\varphi(P)$, де φ — відповідна ізогенія;
- генерація послідовностей. Нові точки на кожній кривій можуть використовуватися для виведення псевдовипадкових чисел. Координати цих точок служать як вихідні дані для генератора ПВП;
- безпека та повторюваність. Оскільки ізогенні перетворення зберігають алгебраїчну структуру, але модифікують параметри кривої, створюється непередбачувана послідовність, яку важко аналізувати атакуючим. Це забезпечує високий рівень безпеки для криптографічних застосувань.

Використовуючи принципи збереження групової структури, можна ефективно маніпулювати елементами еліптичних кривих для створення високого рівня криптографічної стійкості. Схема, представлена на рисунку 1, демонструє модель модифікованого генератору Dual_EC_DRBG.

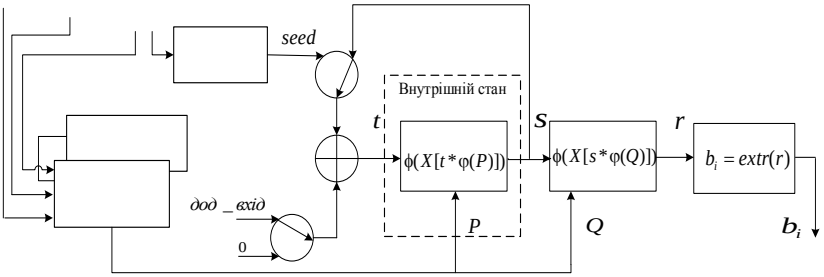


Рис. 1. Модель модифікованого генератору Dual_EC_DRBG

Алгоритм роботи методу генерації ПВП на основі ізогеній еліптичних кривих (додаток Б) можна описати таким чином:

1. Визначення програмної функції генерації ПВП:

```
def generate_large_random_sequence(prime_field, curve_coeffs, isogeny_degree, total_bits=100000, output_file="random_sequence.bin")
```

На цьому етапі визначаються вхідні параметри функції генерації ПВП, а саме:

– *prime_field*: просте число, що задає порядок скінченного поля F_p .

– *curve_coeffs*: коефіцієнти a та b для рівняння еліптичної кривої:

$$y^2 = x^3 + a_{init}\, x + b_{init} \in F_p,$$

де a_{init}, b_{init}, F_p- параметри стандартизованої еліптичної кривої;.

– *isogeny_degree*: ступінь ізогенії *d*.

– *total_bits*: загальна кількість бітів, що мають бути згенеровані (довжина псевдо-випадкової послідовності на виході генератору).

– *output_file*: ім'я файлу для зберігання бітів псевдовипадкової послідовності.

2. Ініціалізація скінченного поля та еліптичної кривої:

```
F = FiniteField(prime_field)
E = EllipticCurve(F, curve_coeffs)
```

На цьому етапі визначається характеристика скінченного поля F_p та еліптична криву *E*

Параметри *prime_field* та *curve_coeffs* можливо реалізувати декількома способами:

– ручне введення

– отримання значень цих параметрів з додаткового файлу

– викликом параметрів стандартизованих ЕК

3. Вибір випадкової точки та її скалярне множення:

```
P = E.random_point()
random_scalar = ZZ.random_element(E.order())
P = random_scalar * P
```

На цьому етапі роботи відбувається генерація базової точки $P(x; y) \in E$, обирається випадковий скаляр *random_scalar* <*ord(E)*, і виконується скалярне множення точки P на згенерований скаляр (*random_scalar*).

4. Генерація параметрів ізогенії та отримання нової ізогенної кривої E':

```
isogeny = E.isogeny(P, degree=isogeny_degree)
E_prime = isogeny.codomain()
```

На цьому етапі генерується ізогенія з використанням заданого ступеня (isogeny_degree) та точки P, що є порядком базової точки P, та отримуємо нову криву E_prime, яка є результатом цього відображеня. Властивості кривої E_prime зберігаються у функції isogeny.codomain().

5. Генерація випадкових бітів:

```
bit_sequence = bytearray()
for _ in range(total_bits):
  Q = E_prime.random_point()
  Q = x_scalar * Q
  while Q.is_zero():
    Q = E_prime.random_point()
  R = x_scalar * Q
  if R.is_zero():
    continue
  x, y = R.xy()
  last_bit = int(x) & h
  bit_sequence.append(last_bit)
```

На цьому етапі генеруються випадкові точки Q_i на новій кривій E_prime. Кожна точка множиться на x -координату точки R_{i-1}, отриманої в попередньому циклі i-1 за модулем порядку цієї точки, і визначається h останніх бітів x - координати точки R для додавання (append(last_bit)) у послідовність бітів bit_sequence.

6. Запис у файл:

```
with open(output_file, 'wb') as file:
  file.write(bit_sequence)
```

На цьому етапі відкривається файл у бінарному режимі на запис (wb) і зберігається бітова послідовність bit_sequence, яка була згенерована.

Таким чином, в ході проведення досліджень розроблено метод генерації псевдовипадкових послідовностей на основі використання ізогеній еліптичної кривої, який відрізняється від відомих методів використанням ізогенного відображення точок кривої на основі секретного ключа (ядра ізогенії). Напрямком подальших досліджень є оцінка статистичної безпеки та оцінка стійкості методу генерації псевдовипадкових послідовностей на основі ізогеній еліптичної кривої до класичного та квантового криптоаналізу.

М.М. Шамко, А.Д. Данилов

АНАЛІЗ ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ

Вступ

Використання блокчейн технологій у сфері енергетики у 2024 році стає все більш актуальним та важливим. Блокчейн дозволяє створювати децентралізовані та прозорі системи, які можуть значно підвищити ефективність, безпеку та надійність енергетичних мереж. Однією з ключових переваг є можливість застосування смарт-контрактів, які автоматизують процеси укладання договорів, розподілу ресурсів та управління потоками енергії, що робить ці процеси більш швидкими та менш витратними.

Цей новий підхід до управління енергоресурсами відкриває безліч можливостей, але водночас ставить перед нами нові виклики, такі як захист від кібератак та інтеграція з існуючими системами. Важливими аспектами, які потребують уваги, є юридичні рамки для смарт-контрактів, технічні засоби для реалізації блокчейн проектів, а також методи захисту критичної інфраструктури від потенційних кіберзагроз. Розглянемо деякі питання, що стосуються впровадження блокчейн технологій у галузі енергетики.

1. Юридичні аспекти використання смарт-контрактів для укладання договорів в сфері енергетики, міжнародний досвід та найкращі практики:

• **Регулювання смарт-контрактів:** Важливість правової визначеності та юридичної сили смарт-контрактів у різних юрисдикціях. Розробка правових рамок для їх використання в енергетичному секторі.

• **Міжнародний досвід:** Огляд законодавства та регуляторних підходів у країнах, які активно впроваджують блокчейн у енергетичний сектор (наприклад, ЄС, США, Китай). Дослідження кращих практик та моделей регулювання.

• **Найкращі практики:** Приклади успішного використання смарт-контрактів для автоматизації розрахунків, управління електропостачанням та торгівлі енергією. Впровадження стандартів та рекомендацій для забезпечення правової та операційної ефективності смарт-контрактів.

2. Аналіз атак на смарт-контракти та захист від них

• **Типи атак:** Аналіз основних загроз, таких як переповнення, рейсингові умови, та вразливості, пов'язані з логікою контрактів. Опис реальних випадків атак на смарт-контракти.

• **Захист від атак:** Використання методів статичного та динамічного аналізу для перевірки безпеки смарт-контрактів, а також найкращі практики кодування. Стратегії для мінімізації ризиків та запобігання вразливостей.

• **Інструменти та технології:** Огляд існуючих інструментів для аудиту смарт-контрактів, таких як MythX, Slither, та інші. Використання автоматизованих систем перевірки та аналізу безпеки смарт-контрактів.

3. Аналіз технічних та програмно-апаратних засобів, необхідних для реалізації проектів, що базуються на використанні блокчейн технологій в енергетиці

• **Технічна інфраструктура:** Необхідні апаратні засоби, такі як сервери, дата-центри та розподілені системи зберігання даних. Вимоги до потужності та продуктивності обладнання.

• **Програмні рішення:** Платформи для розробки та розгортання смарт-контрактів (наприклад, Ethereum, Hyperledger, Corda). Інструменти та середовища для розробки блокчейн додатків.

• **Інтеграція блокчейн:** Виклики та рішення щодо інтеграції блокчейн-технологій з існуючими енергетичними системами та мережами. Впровадження інтерфейсів для взаємодії між різними системами.

4. Аналіз особливостей існуючих та інноваційних рішень в енергетичній галузі, що використовують блокчейн технології

• **Розподілені енергосистеми**: Використання блокчейн для управління розподіленими джерелами енергії та мікромережами. Приклади проектів та ініціатив у цій сфері.

• **Торгівля енергією**: Платформи для p2p торгівлі енергією, що дозволяють споживачам купувати та продавати електроенергію без посередників. Моделі та механізми роботи таких платформ.

• **Трекінг та верифікація:** Системи для відстеження походження енергії та підтвердження її екологічності, використовуючи блокчейн. Важливість прозорості та надійності даних про джерела енергії.

5. Методи кіберзахисту критичної інфраструктури

• **Захист мереж:** Впровадження захищених протоколів для забезпечення безпеки даних в енергетичних мережах. Методи виявлення та запобігання кібератакам.

• **Ідентифікація та аутентифікація**: Системи для надійної аутентифікації користувачів та пристроїв у мережах, що використовують блокчейн. Використання двофакторної аутентифікації та біометричних методів.

• **Моніторинг та реагування:** Інструменти для моніторингу кіберзагроз у реальному часі та системи для швидкого реагування на інциденти. Використання аналітики та машинного навчання для підвищення ефективності захисту.

Висновок

Використання блокчейн технологій в енергетиці у 2024 році демонструє значний потенціал для підвищення ефективності, прозорості та безпеки управління енергоресурсами. Смарт-контракти забезпечують автоматизацію та оптимізацію процесів укладання договорів та розподілу ресурсів, що знижує витрати та покращує оперативність. Проте, впровадження блокчейн технологій в енергетичний сектор супроводжується викликами, такими як необхідність адаптації правових рамок, технічна інтеграція з існуючими системами та захист від кібератак.

Юридичні аспекти використання смарт-контрактів вимагають ретельного опрацювання для забезпечення їх правової сили та сумісності з міжнародними стандартами. Аналіз атак на смарт-контракти та розробка ефективних захисних механізмів є критично важливими для безпеки блокчейн систем. Технічні та програмно-апаратні засоби повинні бути ретельно обрані та інтегровані для забезпечення надійного функціонування блокчейн проектів.

Інноваційні рішення в енергетичній галузі, такі як розподілені енергосистеми та p2p торгівля енергією, показують, як блокчейн може змінити традиційні підходи до управління енергією. Методи кіберзахисту критичної інфраструктури, включаючи захист мереж, ідентифікацію та аутентифікацію, а також моніторинг і реагування на загрози, є ключовими для забезпечення безпеки в умовах зростаючої кількості кіберзагроз.

У підсумку, блокчейн технології відкривають нові горизонти для енергетичної галузі, проте їх ефективне впровадження вимагає комплексного підходу, що включає технічні, юридичні та організаційні заходи. Співпраця між різними секторами та міжнародний обмін досвідом є ключовими факторами успішного використання блокчейн у сфері енергетики, що сприятиме стійкому розвитку та безпеці енергетичної інфраструктури в майбутньому.

1. World Economic Forum. "Blockchain in Energy: A New Paradigm for Decentralized Energy Markets." World Economic Forum, www.weforum.org/whitepapers/blockchain-in-energy-a-new-paradigm-for-decentralized-energy-markets (дата звернення: 30.05.2024)
2. International Energy Agency (IEA). "Blockchain Technology and the Energy Sector: A Review of Research and Development." IEA, www.iea.org/reports/blockchain-technology-and-the-energy-sector (дата звернення: 30.05.2024)
3. CB Insights. "Blockchain in Energy: Transforming the Future of Power." CB Insights, www.cbinsights.com/research/blockchain-energy-power-distributed/ (дата звернення: 30.05.2024)

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2024»

Збірник матеріалів конференції

5 червня 2024 р.

Usage of blockchain technologies in energetics – 2024 : collection of materials of the scientific and practical conference, Kyiv, June 5, 2023, PIMEE of NAS of Ukraine. - 2024. - 36 p.

Використання блокчейн технологій в енергетиці – 2024» 2024 : збірник матеріалів науково-практичної конференції, м. Київ, 5 червня 2024 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2024. – 36 с.