НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

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

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2023»

Збірник матеріалів конференції
28 листопада 2023 р.

Київ – 2023

УДК 620.9: 004(65 + 056.53)
ББК 31
В-43

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 10 від 30 листопада 2023 р.)

ПРОГРАМНИЙ КОМІТЕТ:

В.В. Мохор, доктор технічних наук, професор, член-кор.НАН України,
О.А.Чемерис, доктор технічних наук, професор,
В.В. Чьочь, кандидат технічних наук,
В.О. Артемчук, доктор технічних наук, старший науковий співробітник,
Л.В. Ковальчук, доктор технічних наук, професор

ОРГАНІЗАЦІЙНИЙКОМІТЕТ

В.О. Артемчук, доктор технічних наук, с.н.с.,
Т.М. Клименко,
Г.В. Неласа
О.В.Цуркан

В-43 Usage of blockchain technologies in energetics – 2023: collection of materials of the scientific and practical conference, Kyiv, November 28, 2023, PIMEE of NAS of Ukraine. - 2023. - 72 p.

В-43 Використання блокчейн технологій в енергетиці – 2023 : збірник матеріалів науково-практичної конференції, м. Київ, 28 листопада 2023 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2023. – 72 с.

© Автори публікацій, 2023
© ІПМЕ ім. Г.Є. Пухова НАН України, 2023

ЗМІСТ

S.V. Konovalenko **ADVANTAGES OF USING BLOCKCHAIN IN THE ENERGY INDUSTRY** 5

V.Y. Chevardin, I.V. Lavryk, O.O. Pryima, O.V. Marchuk **CSIDH BENCHMARKING** 8

О.В. Васильєв, В.В. Васильєв **СТРУКТУРНА СХЕМА ІНТЕЛЕКТУАЛЬНОГО ЛІЧИЛЬНИКА СПОЖИВАННЯ ЕНЕРГІЇ, ЩО ІНТЕГРОВАНИЙ ДО БЛОКЧЕЙН МЕРЕЖІ** 11

О.В. Васильєв, В.В. Чьочь **ОЦІНКА ПАТЕНТОЗДАТНОСТІ ТЕХНІЧНИХ РІШЕНЬ ПРИ ВИКОРИСТАННІ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ** 14

Н.В. Заїка, В.С. Ракович, М.Ю. Комаров **ЗАСТОСУВАННЯ ГРУП БПЛА ДЛЯ МОНІТОРИНГУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗЗОВНІ ТА ВСЕРЕДИНІ ПРИМІЩЕНЬ** 16

Г.В. Неласа, А.О. Зайцева, **СМАРТ-КОНТРАКТ ДЛЯ ОПЛАТИ КОМУНАЛЬНИХ ПОСЛУГ** 19

Є.О. Застьола, І.І. Соснов **РОЗГЛЯД МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ КРИПТОВАЛЮТ ДЛЯ ОПТИМІЗАЦІЇ ФІНАНСОВОЇ ЛІКВІДНОСТІ У ЕНЕРГЕТИЧНОМУ СЕКТОРІ** 23

Л.В. Ковальчук, Н.В. Кучинська, М.С. Кондратенко **ВИЗНАЧЕННЯ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ У ДВОРІВНЕВОМУ БЛОКЧЕЙНІ З ПРОТОКОЛОМ КОНСЕНСУСУ PROOF-OF-PROOF ДЛЯ ЗАПОБІГАННЯ АТАКИ ПОДВІЙНОЇ ВИТРАТИ** 25

Л.В. Ковальчук, Н.В. Лисенко **ПЕРЕВАГИ ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ В ЕНЕРГЕТИЦІ ТА ПРОБЛЕМИ, ЯКІ ПОТРІБНО ВИРІШИТИ ДЛЯ ЇХ ВИКОРИСТАННЯ** 29

О.В. Неласий, С.С. Самойлик, Г.В. Неласа **ПЛАТІЖНА СИСТЕМА ДЛЯ СТАНЦІЇ БЕЗДРОТОВОЇ ЗАРЯДКИ ЕЛЕКТРОКАРІВ З ВИКОРИСТАННЯМ СМАРТ-КОНТРАКТІВ** 34

А.А. Макурін **ВИТРАТИ ЕЛЕКТРОЕНЕРГІЇ НА ВИДОБУТОК БІТКОЇНА ТА ТЕХНОЛОГІЯ БЛОКЧЕЙН** 36

Н.О. Маслова, М.О. Рудською **ЕКСПЕРИМЕНТАЛЬНЕ СЕРЕДОВИЩЕ ДЛЯ ДОСЛІДЖЕННЯ ПРОГРАМНОГО КОНТЕНТУ** 40

М.Л. Рафальський **СМАРТ-КОНТРАКТИ В СУЧАСНОМУ ПРАВОВОМУ ПОЛІ: АНАЛІЗ ЮРИДИЧНИХ ВРАЗЛИВОСТЕЙ ТА ВИКЛИКІВ** 43

С.А. Паршенніков, Л.В. Накашидзе **ГЕОТЕРМАЛЬНА ЕНЕРГІЯ: ВИКЛИКИ ТА ІННОВАЦІЇ** 47

О.А. Пащенко, В.Л. Хоменко **ЮРИДИЧНІ ВИКЛИКИ ЗАСТОСУВАННЯ СМАРТ-КОНТРАКТІВ В ЕНЕРГЕТИЦІ** 50

М.Ю. Родінко **ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ПРОТОКОЛІВ КОНСЕНСУСУ BFT В ЕНЕРГЕТИЦІ** 54

О.А. Сергієнко, П.О. Самусь **АНАЛІЗ ПОТОЧНОГО СТАНУ ПРАВОВОГО РЕГУЛЮВАННЯ ЦИФРОВИХ СМАРТ-КОНТРАКТІВ В УКРАЇНІ ТА В СВІТІ** 58

І.О. Усатий, О.М. Любименко, О.А. Штепа **ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ ДЛЯ КОНТРОЛЯ ЕНЕРГЕТИЧНИМИ ПОТОКАМИ В ЕНЕРГОСИСТЕМІ** 61

Д.О. Феденко **БЛОКЧЕЙН ТЕХНОЛОГІЇ В ЕНЕРГЕТИЦІ: СИНЕРГЕТИКА ТА ПРАКТИКА** 63

Чемерис О.А. **ІНФОРМАЦІЙНІ СИСТЕМИ ЕНЕРГЕТИКИ, ПОБУДОВАНІ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН** 65

В.О. Шведов, Ю.І. Рудик, В.Р. Куць **ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОЄКТІВ БЛОКЧЕЙН-ГРІД ЕЛЕКТРОПОСТАЧАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ** 68

S.V. Konovalenko

ADVANTAGES OF USING BLOCKCHAIN IN THE ENERGY INDUSTRY

The concept of a distributed energy system has gained widespread recognition as the most effective way to achieve energy sustainability. It enables the incremental utilization of energy, leading to significant improvements in energy efficiency. With its flexibility and efficiency, a distributed energy system can cater to diverse energy demands in different scenarios. Consequently, the development of distributed energy plays a crucial role in accomplishing the global energy transition [1,4].

Blockchain technology is leading a decentralized revolution, particularly in the realm of energy. The integration of blockchain and energy holds great promise for ensuring future energy sustainability.

Blockchain is a system that enables peer-to-peer interaction in a network without intermediaries and provides direct access to information for all network participants. Due to its structure and operating principles, data tampering is not possible in the system (as it would require massive computational resources that would ultimately be uneconomical).

The working principle revolves around a chain consisting of blocks. Transactions, generated by system users (e.g., money transfers), are grouped into blocks. Each block, in addition to the set of transactions recorded within it, contains a hash value based on the data contained in that block (including the transactions). This hash value is computed using the SHA-2 algorithm. All blocks are arranged in a queue according to their creation order. The current block, in addition to its computed hash value based on its own data, includes the hash value of the previous block. The hash value of the previous block also contributes to the computation of the hash value of the current block. It is this characteristic that forms the chains. Changing even a single character will result in a drastic change in the hash value, which, in turn, will alter the hash values of all subsequent blocks (indicating an attempt to tamper with the data) [3].

Transactions must contain the sender's address, recipient's address, transaction creation time, useful information, and a digital signature. The sender and recipient addresses are user wallets. Addresses are implemented using asymmetric encryption and represented as a public key, which is accessible to all network users. The transaction creation time is represented as a timestamp. To successfully operate in the blockchain network, a user must have a generated pair of public and private keys. With the private key, which is only accessible to the key owner, a digital signature can be created that will match positively when compared to the public key. This process verifies that the public key has not been tampered with.

Another important aspect of blockchain is the process of proof of work (PoW), also known as mining. The hash value of all blocks is adjusted to have a certain number of zeros. The number of zeros is determined by a variable called difficulty. In the process of computing the hash value, another variable called nonce is involved. During mining, the nonce variable is incremented, which leads to the recalculation of the hash value. Recalculation continues until all characters of the hash value fall within the range of and consist of zeros. The mining time increases exponentially with difficulty, allowing for the adjustment of the duration of this process based on the computational power in the network.

After a block has been successfully mined, it is sent to all or a majority of the network participants, each of whom verifies the validity of the chain considering the new block. The essence of verification lies in the recalculation of the hash value for each block. Since a block stores its own hash value and the hash value of the previous block, verification occurs for each block: the stored hash value of the previous block is compared with the hash value of the previous block itself. If the majority or all network participants confirm the successful verification, the block is added to the chain, and all network participants update the chain with the new block.

The system is essentially represented as a decentralized network of nodes for each user with the same functionality depending on their role (system user, miner) and a bootstrap server that performs the infrastructure task of synchronizing users with each other. The bootstrap server contains a collection of users (user pool) in terms of MongoDB [3].

To start working with the system, the user needs to run a server on their local machine that receives requests and processes data (backend server), as well as a server that provides a graphical user interface (front-end server). In the network, there are two roles for users: users who mine blocks and users who create transactions. Each instance of the data processing server and the user interface server pair represents a network node.

During the architecture design, a decision was made to introduce this server to separate responsibilities. The server should perform one and only one task. This is because if changes are made to the software code or new functionality is added, the code can become tightly coupled (in the absence of functional separation), making it difficult to maintain in the future. It was also decided that in the case where the blockchain has no blocks and the network has no users, the bootstrap server creates the first block (genesis block).

Interaction between the user and the bootstrap server takes place to obtain data about other users in the network. The same principle applies to the interaction between the miner and the bootstrap server.

The interaction between the miner and the user involves the miner receiving transactions from the user and after mining a block, broadcasting it to all nodes. If the block passes validation and has not been previously added to the blockchain, it is added, and the miner receives a monetary reward for the work performed.

Compared to traditional energy technologies, the application of blockchain in the energy field offers several technical advantages. Firstly, it enables the establishment of a distributed energy trading and supply system. Blockchain technology supports decentralized energy supply systems and simplified multi-layer systems. This allows power producers, distribution system operators, transmission system operators, and suppliers to directly connect producers and consumers for transactions at all levels through the blockchain network.

Secondly, blockchain technology, combined with smart contracts, enables effective control of energy networks. Smart contracts trigger transactions based on predefined rules, providing a mechanism for controlling energy networks. This automation helps balance supply and demand by ensuring that all energy and storage flows are controlled automatically.

Thirdly, blockchain provides a secure record of all energy flows. Energy blockchain stores transaction data on a single blockchain, creating a distributed and secure record of all energy flows and business activities. This enhances transparency and accountability in the energy sector [2].

In conclusion, the application of blockchain technology in the energy field offers significant technical advantages. It facilitates the development of a decentralized energy trading and supply system, allowing direct transactions between power producers, operators, and consumers at all levels. Additionally, blockchain, in combination with smart contracts, enables effective control and automation of energy networks, ensuring a balance between supply and demand. Moreover, the use of blockchain technology provides a secure and transparent record of all energy flows and transactions, enhancing accountability within the industry. These advantages highlight the potential of blockchain in transforming the energy sector and promoting more efficient and sustainable energy systems.

1. JinM. et al.Microgrid to enable optimal distributed energy retail and end-user demand response Appl. Energy (2018)
2. KamilarisA. et al. The rise of blockchain technology in agriculture and food supply chains Trends Food Sci. Technol. (2019)
3. Nakamoto S. A Peer-to-Peer Electronic Cash System [Електронний ресурс] // Bitcoin. – Режим доступ до ресурсу: https://bitcoin.org/bitcoin.pdf
4. PereraA.T.D. et al.Redefining energy system flexibility for distributed energy system design Appl. Energy (2019)

CSIDH BENCHMARKING

Modern cryptographic systems, traditionally built on mathematical operations involving elliptic curve point groups, are no longer seen as the forefront of information security technology. This shift is primarily due to the advent of quantum computers. The emergence of real quantum computing capabilities has spurred the development of what is known as post-quantum cryptography.

This new era in cryptography is defined by the need to withstand attacks from quantum algorithms like Shor's and Grover's, which can break existing RSA and elliptic curve-based systems on a sufficiently powerful quantum computer (e.g., one with at least 2048 qubits).

As a result, new cryptographic systems are being developed that are believed to be secure against quantum computing attacks. These post-quantum systems typically require much larger key sizes compared to current standards. For example, while a 2048-bit key is standard for RSA today, post-quantum algorithms, like the McEliece-based cryptosystem, demand keys as large as 3211248 bits. Similarly, hash-based signature systems, code-based encryption algorithms, MQ signature system algorithms, lattice-based cryptography (such as NTRU), multivariate quadratic equations cryptography, and secret-key cryptography algorithms all feature significantly larger key sizes.

However, the move to post-quantum cryptography isn't just about larger key sizes; it also involves transitioning from current platforms and software libraries to new ones that can support these advanced cryptosystems. This represents a major challenge in the field.

One promising direction of research in post-quantum cryptography is the development of algorithms based on the isogeny of elliptic curves. These are being explored using existing platforms and software function libraries, adapting them to meet the increased requirements for cryptographic robustness in the age of quantum computing.

One of this group of protocols is alternative to the SIDH (Supersingular Isogeny Diffie-Hellman) protocol - CSIDH (Commutative SIDH) algorithm, which has the shortest known key length. Instead of the extended field F_{p^2}) used in SIDH, operations in CSIDH are carried out in the simple field F_p, which for a given p halves the length of field elements and key sizes.

The general idea of the protocol is that with the help of publicly available parameters Alice and Bob perform separate calculations of isogenies of degree l_A^a and l_B^b, respectively, calculating the isogeny of large order over the secret kernel.

Public CSIDH parameters include:

- A prime number p of the form $l_A^a l_B^b \cdot f \pm 1$, where l_A^a and l_B^b are small prime numbers, a and b are natural integers, and f is a cofactor.
- Supersingular elliptic curve, $E_0(F_p)$.
- Points $\{P_A, Q_A\}$ generated from $E_0[l_A^a]$ over $\mathbb{Z}/l_A^a\mathbb{Z}$ and points $\{P_B, Q_B\}$ generated from $E_0[l_B^b]$ over $\mathbb{Z}/l_B^b\mathbb{Z}$.

The protocol consists of two rounds, which can be divided into following steps:

- Calculating the secret kernel $R = \langle [m]P + [n]Q \rangle$ for base points $\{P, Q\}$, where m and n are private keys.
- Calculation of isogeny over the secret kernel, $\varphi: E \to E/\langle R \rangle$, using the Velu` algorithm for the supersingular curve E.
- Calculate the mappings of the base points of the base of the other side, $\{\varphi(P_{opp}), \varphi(Q_{opp})\}$, for the first round.

Thus, for the first round, Alice and Bob calculate the isogeny $\varphi_A: E_0 \to E_A = E_0/\langle [m_A]P + [n_A]Q \rangle$. They apply isogeny to the base points of the other side. After the first round, Alice sends Bob $(E_A, \{\varphi_A(P_B), \varphi_A(Q_B)\})$. Bob sends Alice $(E_B, \{\varphi_B(P_A), \varphi_B(Q_A)\})$ through unprotected chanel. The second round consists of a similar calculation of isogeny, but with the public keys they exchanged. Alice calculates $\varphi'_A: E_B \to E_{AB} = E_B/\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$, Bob calculates $\varphi'_B: E_A \to E_{BA} = E_A/\langle [m_B]\varphi_A(P_B) + [n_B]\varphi_A(Q_B) \rangle$ to obtain a general secret, Alice calculates the j-invariant of E_{AB},and Bob of E_{BA}.

The safety assumption is based on the difficulty of calculating isogeny between supersingular elliptic curves for which there is no subexponential algorithm known for quantum computers. Alice generates private keys $m_A, n_A \in \mathbb{Z}/l_A^a\mathbb{Z}$, which are not divisible by l_A^a. Bob also generates private keys $m_B, n_B \in \mathbb{Z}/l_B^b\mathbb{Z}$, which are not divisible by l_B^b .

An evaluation of the speed of algorithm execution on processors of different types, architectures and purposes was also carried out (Table 1). A cryptographic library written in Go, specifically the “cloudflare/circl/dh/csidh” package. These benchmarks measure the performance of various cryptographic operations, such as key generation, validation, and arithmetic operations on elliptic curves and finite fields.

Here's a summary of the key benchmarks:

1. “GeneratePrivate”: Measures the time taken to generate a private key.
2. “GenerateKeyPair”: This measures the key pair generation time.
3. “ValidateRandom”: A very fast validation check for random data.
4. “ValidateGenerated”: This is similar to the Validate test but for generated keys.
5. “Derive”: It measures the time taken for key derivation.
6. “DeriveGenerated”: It measures the time taken for key derivation.

7. “XMul, XAdd, XDbl, Isom”: These benchmarks are related to elliptic curve arithmetic.
8. “Fp (sub512, mul, cswap, add, sub, mul#01, exp)”: These benchmarks test finite field operations

These benchmarks were running on an Intel Xeon Gold 6338 CPU with 5 vCPUs with Linux OS, Intel Core i5-8300H with Windows OS, Intel Core i9-11900H with Windows OS and M1 Pro Max with macOS. All benchmarks are measured in ns/op (nanoseconds per opration).

Table 1 – Benchmark results

Benchmark	**Core i5 8300H**	**Xeon Gold 6338 (5 vCPU)**	**Core i9 11900H**	**M1 Pro Max**
GeneratePrivate	13,078	39,845	10,152	20,036
GenerateKeyPair	41,225,325	72,602,410	29,284,254	63,558,393
ValidateRandom	318.4	1,063	203.8	617.4
ValidateGenerated	43,028,672	77,619,708	32,139,783	68,169,292
DeriveGenerated	121,471,467	231,220,253	94,176,008	197,038,785
XMul	442,616	825,684	333,542	712,006
XAdd	451.1	835.7	340.2	703.2
XDbl	512.0	954.2	388.7	821.8
Isom	13,980	25,125	10,492	23,906
Fp/sub512	3.703	7.263	3.001	2.756
Fp/mul	5.330	6.973	3.044	3.127
Fp/cswap	4.884	6.607	3.364	5.349
Fp/add	9.480	17.49	8.361	7.252
Fp/sub	10.39	15.61	7.273	5.134
Fp/mul#01	65.56	111.2	49.27	110.8
Fp/exp	42,822	80,876	32,483	73,457

The comprehensive benchmarking of the CSIDH algorithm, as part of the evolving landscape of post-quantum cryptography, reveals insights into its performance across various computing platforms. Our analysis, conducted on processors with differing architectures and purposes, underscores the robustness and efficiency of CSIDH, particularly in the context of its key generation, validation, and cryptographic operations on elliptic curves and finite fields. Results of this test will be useful for organizations, who are trying to implement PKI and carrying out a research on hardware and software for it.

Moving forward, it is imperative to continue exploring and refining such post-quantum cryptographic algorithms. The development algorithms based on the isogeny of elliptic curves like CSIDH, represents a critical stride towards securing information systems against the rapidly evolving capabilities of quantum computing. The benchmarks presented in this study provide a foundational understanding of CSIDH's performance, setting the stage for further optimization and implementation in real-world applications.

О.В. Васильєв, В.В. Васильєв

СТРУКТУРНА СХЕМА ІНТЕЛЕКТУАЛЬНОГО ЛІЧИЛЬНИКА СПОЖИВАННЯ ЕНЕРГІЇ, ЩО ІНТЕГРОВАНИЙ ДО БЛОКЧЕЙН МЕРЕЖІ

Інтелектуальний лічильник з інтеграцією в блокчейн-мережу – це вдосконалений тип лічильника енергії, який може записувати та зберігати дані про споживання енергії в блокчейні. Інтеграція технології блокчейн в інтелектуальний облік приносить кілька потенційних переваг:

1. Безпека даних: використання блокчейну може підвищити безпеку даних, що записуються розумними лічильниками. Оскільки структури даних блокчейна є незмінними та стійкими до втручання, дані про споживання енергії, записані в них, менш сприйнятливі до шахрайства чи кібератак.

2. Прозорість і достовірність: децентралізований характер блокчейна означає, що всі транзакції є прозорими та доступними для перевірки всіма сторонами в мережі. Це може підвищити довіру споживачів, комунальних компаній і регуляторів.

3. Однорангова торгівля енергією: розумні лічильники з інтеграцією блокчейну можуть полегшити однорангову (P2P) торгівлю енергією. Споживачі з надлишковою енергією, можливо, отриманою з відновлюваних джерел, таких як сонячні батареї, можуть продавати її безпосередньо іншим споживачам без необхідності центрального посередника.

4. Точне виставлення рахунків і дані в режимі реального часу: блокчейн може надати перевірений і точний облік споживання енергії, який можна використовувати для цілей виставлення рахунків у режимі реального часу, допомагаючи усунути помилки виставлення рахунків і створюючи більш динамічні моделі ціноутворення.

5. Автоматизація контрактів: у поєднанні зі смарт-контрактами блокчейн може автоматизувати багато процесів. Наприклад, комунальні платежі можуть бути автоматично активовані, коли виконуються певні умови, наприклад, коли платіж підлягає сплаті, коли було спожито певну кількість енергії.

6. Розподілене управління енергетичними ресурсами: інтелектуальні лічильники в мережі блокчейн можуть сприяти управлінню розподіленими енергетичними ресурсами, забезпечуючи точний і безпечний обмін даними, що є життєво важливим для збалансування попиту та пропозиції в режимі реального часу.

7. Відповідність нормативним вимогам і звітність: незмінні можливості блокчейну для ведення записів можуть допомогти комунальним компаніям у дотриманні нормативних вимог, забезпечуючи аудиторський слід виробництва, споживання та транзакцій енергії.

Інтелектуальний лічильник: фізичний пристрій, підключений до будинку чи підприємства, який вимірює споживання електроенергії, газу чи води. Він має здатність передавати дані майже в реальному часі та може виконувати просту логіку (наприклад, увімкнення чи вимкнення на основі певних умов).

Спрощена структура інтелектуального лічильника складається з наступних структурних модулів:

1. Мікроконтролер/процесор: *всередині інтелектуального лічильника є мікроконтролер або процесор, який керує збором даних, обміном даними та, можливо, простими завданнями обробки.*

2. Датчики вимірювання: *ці модулі збирають дані про використання, напругу, струм тощо та є важливими для основної функції інтелектуального лічильника – вимірювання споживання.*

3. Модуль зв'язку: *він дозволяє інтелектуальному лічильнику надсилати та отримувати дані. Це може бути бездротовий модуль, що використовує такі технології, як Wi-Fi, GSM, LoRaWAN, або в деяких випадках це може бути дротове мережеве з'єднання.*

4. Інтерфейс блокчейну: *це модуль програмного забезпечення в інтелектуальному лічильнику або пов'язаній інфраструктурі, яка взаємодіє з блокчейном. Відповідний алгоритм (та програмний код) включає форматування даних (перетворення показань лічильників у формат, який можна записати в блокчейн), шифрування (захист даних перед їх надсиланням у блокчейн), інформаційнв структура, що реалізує запис про смарт-контракт, модуль обробкиплатежів на основі споживання енергії.*

5. Мережа блокчейну: *централізована та розподілена база даниї, яка фіксує всі транзакції та дані, надіслані з розумних лічильників. Така база даних може бути загальнодоступною (наприклад – Ethereum [1]), коли будь-який авторизований користувач може приєднатися до мережі, як-от Ethereum, що може полегшити торгівлю енергією P2P, або блокчейн консорціуму, коли лише група попередньо схвалених сторін може брати участь у мережі, що може бути більш придатним для комунальних компаній.*

6. Модуль альтернативного зберігання даних: *хоча блокчейн зберігатиме транзакції, додаткове сховище даних може використовуватися для великих наборів даних, які неможливо зберігати в ланцюжку через розмір або вартість. Це може включати децентралізовані рішення для зберігання, які взаємодіють з блокчейном.*

8. Інтерфейс користувача: *платформа для взаємодії користувачів із даними інтелектуального лічильника, перегляду транзакцій та керування своїми рахунками. Це може бути веб-портал або мобільний додаток.*

9. Модуль контролю даних: *Спеціальний модуль який забезпечує гарантії відповідності всіх даних та транзакцій законам і нормам, які регулюють звітність про енергію та транзакції.*

Розумний лічильник з інтеграцією блокчейну зазвичай працює таким чином:

Розумний лічильник збирає дані про споживання через регулярні проміжки часу. Такі дані обробляються та шифруються з допомогою мікроконтролером відповідно до спеціального алгоритму. Через комунікаційний модуль дані надсилаються до мережі блокчейн, де потрапляють у систему смарт-контрактів, які автоматично фіксують дані можуть автоматично перевіряти та записувати дані у відповідну БД та виконувати транзакції на основі використання енергії. Споживачі та комунальні підприємства мають доступ до цих даних через інтерфейс користувача відповідного рівня для моніторингу, виставлення рахунків або торгівлі.

Загалом, інтеграція інтелектуальних лічильників із технологією блокчейн потенційно може трансформувати енергетичний сектор, зробивши його більш безпечним, ефективним і зручним для споживачів, відкриваючи шлях до більш стійких і децентралізованих енергетичних систем. Однак технологія все ще є відносно новою та знаходиться на стадії розробки, і є проблеми, які необхідно вирішити, такі як масштабованість, нормативне середовище та технологічна стандартизація.

1. Zhao, Wenbing, Quan Qi, Jiong Zhou, and Xiong Luo. 2023. "Blockchain-Based Applications for Smart Grids: An Umbrella Review" *Energies* 16, no. 17: 6147. https://doi.org/10.3390/en16176147

О.В. Васильєв, В.В. Чьочь

ОЦІНКА ПАТЕНТОЗДАТНОСТІ ТЕХНІЧНИХ РІШЕНЬ ПРИ ВИКОРИСТАННІ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ

Більшість напрямів застосування блокчейн технологій в енергетиці безумовно відноситься до способів організації розрахунків за споживання енергії, створенню розподілених баз даних для фіксації інформації про функціонування енергетичних мереж та економічної діяльності суб'єктів ринка, алгоритмів шифрування даних, питань комп'ютерної безпеки. Більшість таких рішень і технологій, за деякими виключенням відносяться до сфери авторського права і, за визначенням, не є патентоздатними [1].

Проте застосування блокчейн технологій в секторі реалізації Smart Grid систем та Internet of Thing (Інтернет речей) у формі технічних рішень активно патентуються.

Інформаційною базою для дослідження і аналізу тенденцій патентування є патентний пошук з подальшим застосуванням статистичних та кластерних методів обробки великих масивів даних.

На основі масиву зареєстрованих винаходів (результату інформаційного пошуку у БД Patbase [2] за допомогою пошукової формули (1), обсяг якого складає 2487 патентів (що об'єднуються у 1114 патентних сімейств на кінець листопада 2023 року був проведений контент аналіз і кластеризація тематики вибраних документів.

TAC=(blockchain and
("Smart GRID" OR "Smart-Grid" OR IoT OR "internet of thing"))" *(1)*

Хронологічна динаміка патентування за останні 10 років представлена на Рисунку 1, де повний діапазон складає 16 років, але значне зростання їх кількості спостерігається починаючи з 2014 року. В інтервалі 2014 -2019 року темпи такого зростання збільшилися на 400 відсотків і в останні роки (2020-2022 рік) стабілізувався на рівні 350 заявок на рік. Це дає підстави стверджувати про суттєві перспективи технічної реалізації подібних технологій, інноваційне зростання яких ще знаходиться на начальному етапі росту.

Початковий кластерний аналіз дає можливість визначення Топ5 компаній заявників, у послідовності IBM (переважає інших в 3 рази маючи у власності 32), Siemens AG, Intel, Chaeryeong (KR), Chitkara University (IN) (всі мають по 10 патентів). За географічним фактором загальний рейтинг патентів дає таку послідовність: Індія та США на рівні 400 патентів, КНР (225 патентів), Південна Корея (175 патентів), Австралія-Німеччина- Японія (біля 50 патентів кожна країна)

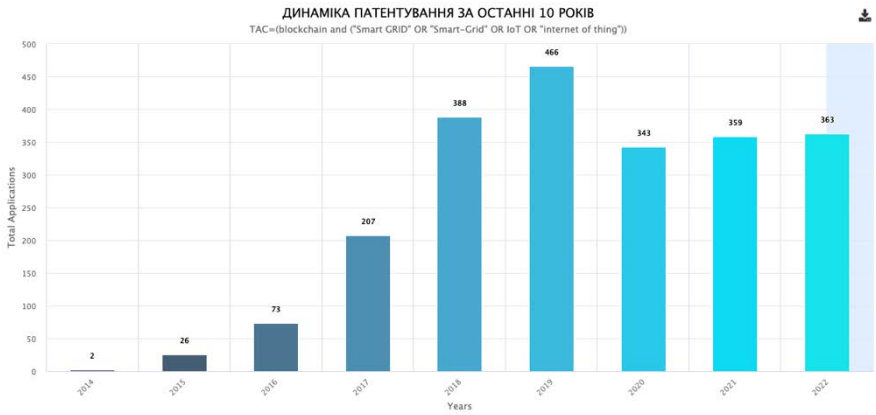

Рисунок 1. Хронологічна динаміка патентування
відповідно пошукової формули (1)

Аналіз тенденцій технічної реалізації вказують на те, що блокчейн розглядається як перспективна технологія, що сприятиме розвитку енергетичної системи майбутнього, сприяючи інноваціям у способах виробництва, розподілу та споживання енергії. Однак впровадження блокчейну в Smart Grid та Internet of thing все ще знаходиться на ранніх стадіях і стикається з різними проблемами технічного порядку.

1. Закон України Про охорону прав на винаходи і корисні моделі. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3687-12#Text
2. PatBase - The Global Patent Database. Minesoft Company. [Електронний ресурс]. – Режим доступу: https://www.patbase.com/pb202009.pdf

Н.В. Заїка, В.С. Ракович, М.Ю. Комаров

ЗАСТОСУВАННЯ ГРУП БПЛА ДЛЯ МОНІТОРИНГУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗЗОВНІ ТА ВСЕРЕДИНІ ПРИМІЩЕНЬ

Безпілотні літальні апарати стали невід'ємним інструментом для багатьох фахівців. БПЛА зараз використовується, як для професійної фото та відеозйомки, так і для аматорського спорту.

Багато сучасних компаній займаються розробкою та експлуатацією таких рішень. Однією з основних параметрів всіх апаратів роторного типу є час польоту. Для збільшення часу польоту встановлюють спеціальний набір рухового апарату, наприклад, такий апарат заправляється бензином і генератор виробляє електроенергію, і під заряджає батарею в процесі польоту. Сьогодні такі літальні апарати здатні здійснювати вильоти від 4 годин і більше.

Ринок безпілотних літальних апаратів постійно розвивається. Сьогодні ключовими галузями їх застосування є:

- аерофотозйомка, спорт, навчання;
- картографія та геодезія, моніторинг будівництва;
- агробізнес, вантажоперевезення, аеротаксі;
- військові, ударні, розвідувальні та інші.

Найбільшої популярності набули мультироторні БПЛА. Конструкція та висока мобільність автономних літальних апаратів дозволяють оминати перешкоди, маневрувати у лісі, а також виконує специфічні складні завдання. Деякі з них збираються вручну, інші виробляються у промислових масштабах, такі апарати за своєю природою є автономними і можуть керуватися без втручання оператора в процес керування польотом.

Для розуміння роботи систем управління польотом БПЛА мультироторного типу розглянемо принцип виконання завдання польоту програмними модулями.

БПЛА включає 4 програмні модулі:

- система управління літальним апаратом, яка дозволяє нам контролювати наш апарат та здійснювати дослідження із заданої траєкторії.
- навігаційна система, яка дозволяє зрозуміти та визначити його місце розташування щодо будь-якої системи координат,
- система побудови карти, яка дозволяє нашому літальному апарату орієнтуватися в невідомих умовах та виявляти об'єкти на шляху прямування.
- система планування маршруту, що дозволяє ефективно побудувати маршрут літального апарату, щоб він не зіткнувся з будь-якими об'єктами, а також виконав свою місію максимально ефективно.

В умовах реальної роботи, через жорсткі умови експлуатації, присутності оператора не завжди можливо. Наприклад, при польоті в

приміщеннях, особливо за умови низької освітленості, виникає необхідність високої кваліфікації та навичок пілотування в ручному режимі. Часто у складних завданнях виникають вимоги до автономної роботи навігаційного комплексу, що управляє. Застосування автономних систем та спеціальних автопілотів – дозволяє здійснювати весь цикл польоту від зльоту до посадки, без участі оператора.

Автопілот - це пристрій, який дозволяє керувати БПЛА, і дозволяє абстрагуватись оператору від прямого керування силовою установкою. Задавши параметри траєкторії, автопілот самостійно передає команди керування приводами двигуна. Тобто автопілот отримавши команди від оператора - далі, зробивши внутрішні обчислення, керує БПЛА [1].

Для створення таких комплексів управління - потрібна синхронна робота великої кількості бортових приладів та обладнання. Зазвичай виділяють кілька областей, у яких від апаратів потрібна автономність, це такі завдання як: Шоу дронів, інспекція приміщень, моніторинг об’єктів, доставка вантажів, наукові дослідження, групові спортивні польоти та інше.

- Промисловий моніторинг. Куди входить моніторинг промислових об'єктів будівель, лінії електропередач, вишок стільникового зв'язку, об’єктів критичної інфраструктури тощо.

- Інспекція приміщень, включає такі завдання як дослідження небезпечних для людини приміщень, огляд промислового обладнання і техніки, створення мапи приміщень або конструкції будівлі при рятувальних роботах (при пошкодженні існуючих конструкцій та об’єктів на території), і так далі.

Для обхвату більшої території можливо використовувати декілька БПЛА одночасно, але в цьому випадку бажано застосовувати рій. Рій складається з кількох автономних дронів, які працюють разом для досягнення мети. Кожен дрон у групі може злітати, приземлятися та зависати. Дрони організовані в шари, які називаються кластерами, і один із дронів обирається лідером рою для зв’язку з наземним диспетчером. Кожен дрон може спілкуватися з лідером зграї та дронами того самого кластера, щоб обмінюватися інформацією. Зв'язок між дронами допомагає безпілотникам коригувати свою поведінку у відповідь на дані в реальному часі [2].

Технологію блокчейн можна використовувати для досягнення прозорого та високонадійного глобального прийняття рішень роєм, яке можна перевірити. Наприклад, безпечне голосування за допомогою блокчейну може допомогти зграї дронів прийняти глобальне рішення.

Захищений і контрольований рій можна використовувати для дистанційного моніторингу рятувальних операцій у певній місцевості. Ройові послуги можуть включати спостереження, зондування та логістику для постраждалих районів. Рій може складатися з різнорідних дронів, якими володіють і керують різні партнери. Катастрофи та стихійні лиха, такі як

землетруси, можуть пошкодити мережеву інфраструктуру, що призводить до обмеження зв'язку між рятувальними командами.

Вміння використовувати БПЛА при огляді конструкцій будівлі об'єктах критичної інфраструктури (ОКІ) [3], дозволяє проводити періодичний моніторинг території ОКІ, виконувати рятувальні роботи, створювати візуальне відображення реального стану будівлі ззовні та внутрішніх приміщень будівлі. Технологію блокчейн можна використовувати для досягнення прозорого та високонадійного глобального прийняття рішень роєм БПЛА.

1. Igor Korobiichuk, Yuriy Danik, Oleksyj Samchyshyn The estimation algorithm of operative capabilities of complex countermeasures to resist UAVs // Simulation: Transactions of the Society for Modeling and Simulation Innternational, 7 August 2018, vol. 95, pp. 569 – 573. DOI: 10.1177/0037549718791264.
2. Перспективи військового застосування технології блокчейну Опірський Іван, Василишин Святослав DOI: 10.18372/2225-5036.28.16950
3. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К. : НІСД, 2019. – 224 с.

Г.В. Неласа, А.О. Зайцева,

СМАРТ-КОНТРАКТ ДЛЯ ОПЛАТИ КОМУНАЛЬНИХ ПОСЛУГ

Смарт-контракти мають потенціал змінити різні галузі, такі як роздрібна торгівля, ланцюг постачання, промисловість та інші, шляхом прискорення транзакцій, зменшення паперової роботи та підвищення прибутковості.

Мета даної роботи полягає в створенні прототипу програмного забезпечення платіжної системи на основі смарт-контрактів на Solidity, за допомогою якого можна спростити процес сплати комунальних платежів.

Переваги використання смарт-контрактів:

- уникнення посередників, а також зменшення формальностей та витрат, пов'язаних з традиційними методами із збереженням надійності, безпечності та автентичності.
- спрощення бізнес-процесів при взаємодії між анонімними автентифікованими сторонами;
- забезпечення більшої безпеки завдяки використанню технології блокчейн, на якій базуються контракти;
- майже миттєве виконання угод для всіх сторін, як тільки необхідні умови будуть виконані;
- створення середовища прозорості та довіри, де всі учасники можуть переглядати інформацію про контракт у блокчейні;
- уникнення необхідності утримання великої компанії в ролі довіреної сторони, оскільки смарт-контракти розподілені між тисячами комп'ютерів, що допомагає уникнути бюрократії, цензури та пов'язаних з цим процесів великих витрат часу.

Ethereum – це децентралізована розподілена обчислювальна платформа з відкритим кодом, яка дозволяє створювати смарт-контракти та децентралізовані програми, також відомі як DApps [1].

В ході виконання роботи реалізовано смарт-контракт розрахунку та сплати за спожиту електроенергію на мові програмування Solidity, за допомогою якої здійснюється програмування смарт-контрактів для блокчейн-платформи Ethereum, а також інтерфейс взаємодії із смарт-контрактом на основі HTML та CSS (рисунок 2).

Розглянемо проект системи. Базовими варіантами використання є "Надання послуг населенню" та "Оплата за електроенергію". Для виконання другого варіанту використання, система звертається до додаткових сервісів "Розрахунок платежу за показаннями" та "Проведення платежу". На рисунку 1 наведено варіанти використання системи оплати. Текстовий сценарій доповнює діаграму, розкриваючи зміст окремих дій, які виконуються системою та акторами в процесі оплати послуг (таблиці 1-3). В головному розділі сценарію (табл. 1) вказується ім’я варіанту використання,

який розглядається, імена взаємопов'язаних з ним акторів, ціль виконання варіанта, посилання на інші варіанти використання.

Рисунок 1 – Діаграма варіантів користування для системи оплати послуг

В наступному розділі сценарію (табл. 2) йде опис послідовності дій, що приводить до успішного виконання варіанту використання, що розглядається. Ініціатором дій виступає один з акторів, в даному випадку – Споживач. Для зручності наступних посилань кожна дія позначається порядковим номером в послідовності.

Таблиця 1 – Головний розділ

Варіант використання	Оплата за електроенергію
Актори	Споживач, Підприємство
Ціль	Проведення успішного платежу
Короткий опис	Споживач робить запит на отримання послуг. Після сплачує за обсяг послуг, які використав.
Посилання на інші варіанти використання	Включає в себе варіанти використання: - розрахунок платежу за показаннями; - проведення платежу.

Таблиця 2 – Розділ "Типовий хід подій"

Типовий хід подій	
Дія акторів	Відгук системи
1. Запит на отримання послуг в сфері електроенергії.	2. Обробка запиту. 3. Надання послуги в сфері електроенергії.
4. Користування послугою.	5. Обробка значень, отриманих від користувача. 6. Розрахунок платежу за значеннями.
7. Проведення платежу. Виняток №1: Недостатньо грошей на рахунку споживача.	8. Обробка отриманого платежу.

В третьому розділі сценарію (табл. 3) йде опис послідовності дій, які виконуються при виняткових ситуаціях (винятків).

Таблиця 3 – Розділ "Винятки"

Дія актора	Відгук системи
Виняток №1. Недостатньо грошей на рахунку споживача	
1. Платіж не проводиться через недостатню кількість грошей на рахунку споживача.	2. Обробка даних. 3. Внесення суми боргу в наступний платіж.
4. Проведення платежу з погашенням боргу.	5. Обробка отриманого платежу.

Нижче наведено код реалізації смарт-контракту для системи оплати за електроенергію EnergyPayment.sol на мові програмування Solidity та інтерфейс платіжної системи (рисунок 2).

```
        // SPDX-License-Identifier: MIT
        pragma solidity ^0.8.18;
        contract EnergyPayment {
        address private owner;
        uint public rate; // вартість одиниці енергії
        struct Consumption {
        uint amount; // кількість спожитої енергії
        uint cost; // вартість спожитої енергії
        bool paid; // чи оплачено споживання
        }
        mapping(address => Consumption[]) public consumptions;
        constructor(uint _rate) {
        owner = msg.sender;
        rate = _rate;
        }
        modifier onlyOwner {
        require(msg.sender == owner, "Caller is not owner");
        _;
        }
        function changeRate(uint _rate) public onlyOwner { // Зміна вартості одиниці енергії
        rate = _rate;
        }
        function recordConsumption(uint _amount) public { // Запис спожитої енергії
        Consumption memory newConsumption;
        newConsumption.amount = _amount;
        newConsumption.cost = _amount * rate;
        newConsumption.paid = false;
        consumptions[msg.sender].push(newConsumption);
        }
        function payConsumption(uint _index) public payable { // Оплата спожитої енергії
        require(!consumptions[msg.sender][_index].paid, "Consumption already paid");
        require(msg.value == consumptions[msg.sender][_index].cost, "Incorrect value transferred");
        consumptions[msg.sender][_index].paid = true;
        }
        function withdrawFunds(uint _amount) public onlyOwner { // Вивести кошти власнику
        payable(owner).transfer(_amount);
        }
}
```

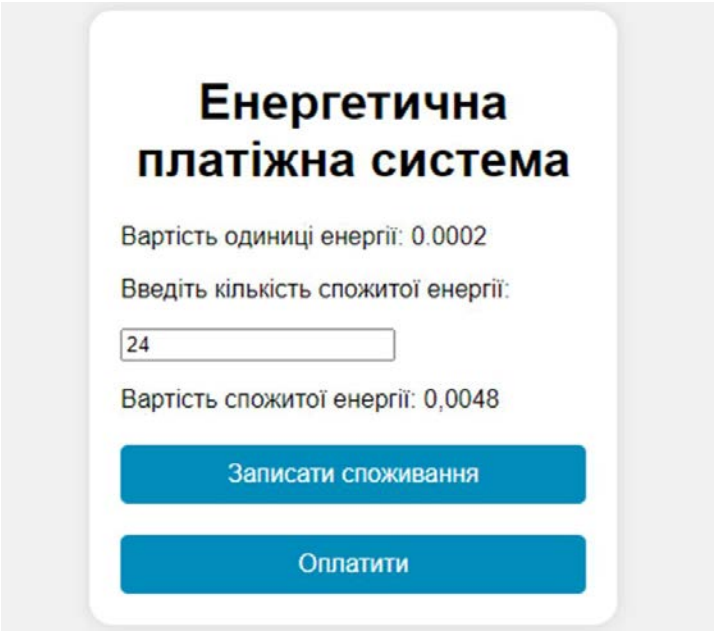

Рисунок 2 – Інтерфейс системи оплати

В результаті роботи отримано працюючий прототип системи оплати за спожиту електроенергію, розроблений за технологією WEB3, що реалізована із використанням смарт-контракту на Solidity, криптогаманця MetaMask для здійснення оплати та інтерфейсу (сайту) на HTML, CSS та JAVA-SCRIPT.

1. «What is Ethereum?» ConsenSys – Електронний ресурс – Режим доступу: https://consensys.net/knowledge-base/ethereum/
2. Nick Szabo «Smart Contracts: Building Blocks for Digital Markets» – Електронний ресурс – Режим доступу: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Є.О. Застьола, І.І. Соснов

РОЗГЛЯД МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ КРИПТОВАЛЮТ ДЛЯ ОПТИМІЗАЦІЇ ФІНАНСОВОЇ ЛІКВІДНОСТІ У ЕНЕРГЕТИЧНОМУ СЕКТОРІ

За останні десятиліття енергетичний сектор став предметом різноманітних інновацій та перетворень, зокрема відмітного зростання зацікавленості використання криптовалют для оптимізації фінансової ліквідності. Однією з ключових проблем, яку ставлять перед собою учасники ринку енергетики, є необхідність залучення інвестицій та ефективне управління фінансовими ресурсами. У цьому контексті криптовалюти представляють собою новий підхід до розв'язання цих завдань, пропонуючи інноваційні рішення та можливості для оптимізації фінансового обігу в енергетичній сфері.

У сучасному енергетичному секторі спостерігається необхідність удосконалення фінансової ліквідності для забезпечення стійкості та розвитку підприємств. Одним із потенційних інструментів для досягнення цієї мети є використання криптовалют, які можуть внести істотні зміни у фінансовий ландшафт енергетичного сектору.[1]

Першочерговим завданням є ретельний аналіз проблем, пов'язаних із фінансовою ліквідністю в енергетичній галузі. Затримки у фінансуванні, складні процеси взаєморозрахунків та зменшення прибутковості стають перешкодою для ефективного управління ресурсами та розвитку інновацій.[2]

Криптовалюти, такі як Bitcoin та Ethereum, володіють потенціалом полегшити фінансові операції в енергетичному секторі. Технологія блокчейн, яка лежить в основі криптовалют, може сприяти автоматизації процесів, зниженню витрат та прискоренню розрахунків між сторонами.

Розгляд вигід використання криптовалют включає зменшення транзакційних витрат, підвищення швидкості та безпеки грошових переказів, а також створення нових моделей фінансування через Initial Coin Offerings (ICO). Крім того, використання криптовалют може допомогти уникнути валютних ризиків при міжнародних трансакціях.

Необхідно ретельно розглянути можливі ризики та виклики, пов'язані з використанням криптовалют в енергетичному секторі, такі як волатильність цін, регуляторні обмеження та можливість використання для незаконних операцій.[3]

На основі аналізу можливостей використання криптовалют для оптимізації фінансової ліквідності в енергетичному секторі, можна зробити висновок, що їх впровадження може стати перспективним інструментом для покращення фінансової стабільності та збільшення ефективності управління ресурсами в даній галузі. Важливо враховувати ризики та ефективно

управляти ними, але при правильному впровадженні криптовалют можуть сприяти створенню більш стійкого та інноваційного енергетичного сектору.

За всіма перевагами та можливостями, які пропонує використання криптовалют у фінансах енергетичного сектору, також важливо врахувати їхню роль у сприянні інноваційному розвитку та стимулюванні інвестицій. Криптовалюти можуть стати каталізатором для створення нових технологій, які покращать ефективність та екологічні показники виробництва енергії.

Зокрема, відкритий та децентралізований характер криптовалют може сприяти розвитку смарт-контрактів, що в свою чергу спростить автоматизацію угод та взаєморозрахунків між енергетичними компаніями. Це дозволить ефективніше використовувати ресурси та зменшити адміністративні витрати.

Таким чином, використання криптовалют у фінансовій сфері енергетичного сектору може визначити новий етап розвитку, сприяючи не лише оптимізації фінансової ліквідності, але й впровадженню інновацій та створенню стійкого та зеленого енергетичного майбутнього.

1. Міністерство енергетики України. Електронний доступ - https://www.mev.gov.ua/
2. Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг. Електронний доступ - https://www.nerc.gov.ua
3. Звіти та дослідження аналітичної компанії Deloitte. Електронний доступ - https://www2.deloitte.com/

Л.В. Ковальчук, Н.В. Кучинська, М.С. Кондратенко

ВИЗНАЧЕННЯ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ У ДВОРІВНЕВОМУ БЛОКЧЕЙНІ З ПРОТОКОЛОМ КОНСЕНСУСУ PROOF-OF-PROOF ДЛЯ ЗАПОБІГАННЯ АТАКИ ПОДВІЙНОЇ ВИТРАТИ

1. Вступ.

У роботі розглядаються питання безпечного функціонування дворівневого блокчейну [1] зі складним змішаним протоколом консенсусу – Proof-of-Stake [2] в основному блокчейні (який ми називаємо мейнчейном) та Proof-of-Work [3] в сайдчейні. Цей дворівневий блокчейн побудовано за принципом протоколу Proof-of-Proof, коли стійкість сайдчейну забезпечується стійкістю мейнчейну, шляхом посилання блоків мейнчейну на блоки сайдчейну з використанням спеціальних транзакцій. Така структура дозволяє швидше випускати блоки у сайдчейні і, відповідно, швидше обробляти транзакції без зниження стійкості та без збільшення об'єму блоку.

Такі дворівневі (каскадні) блокчейни можуть використовуватись як для побудові каскадних державних реєстрів [4], так і в якості безпечного середовища для розміщення смарт-контрактів, зокрема p2p-продажу зеленої енергетики.

Постановка задачі.

Розглядається *дворівневий* блокчейн з протоколом консенсусу Proof-of-Proof [1], у якого у основному блокчейні використовується протокол PoS, а в сайдчейні – PoW. Нехай деяка транзакція, що перераховує кошти вендору, була включена в якийсь блок B_0 сайдчейну. Через деякий час після цього у мейнчейні з'являється посилання на блок B_0, тобто блок $B*$, до заголовку якого входить або геш-значення від блоку B_0, або геш-значення якогось з наступних блоків сайдчейну, яких безпосередньо або опосередковано посилається на блок B_0. У такій ситуації атака подвійної витрати на сайдчейн стає можливою лише за умови, що така атака відбулась у мейнчейні після виходу блоку $B*$.

Задача полягає в наступному: для заданого маленького значення $\varepsilon \in (0, 1)$*, визначити таку найменшу кількість* $\boldsymbol{Z}$ *блоків підтвердження у сайдчейні* (*після першого посилання на блок* B_0 *у мейнчейні, тобто після виходу блоку* $B*$)*, що після їх виходу імовірність атаки подвійної витрати на блок* B_0 *не перевищує задане* $\varepsilon \in (0, 1)$.

Аналогічна задача була повністю розв'язана для дворівневого протоколу консенсусу Proof-of-Proof для таких випадків:

- коли в обох блокчейнах (в основному блокчейні і в сайдчейні) однаковий протокол консенсусу PoW [5] або PoS [6];

В цій роботі ми розглядаємо цю задачу у тому випадку, коли в основному блокчейні протокол консенсусу PoS, а в сайдчейні протокол консенсусу PoW.

2. Допоміжні твердження.

Ми робимо припущення на користь зловмисника, і надалі вважаємо, що:

- всі зловмисники консолідовані, можуть миттєво обмінюватись повідомленнями;

- у основному блокчейні, доля зловмисника (тобто сума стейків всіх нечесних стейкхолдерів) дорівнює p_M (нижній індекс M від англійського слова *malicious*), доля чесних слотлідерів дорівнює p_H (нижній індекс H від англійського слова *honest*), причому $p_M + p_H = 1$ і $p_M < p_H$;

- у сайдчейні, доля зловмисника (тобто сума обчислювальних потужностей всіх нечесних стейкхолдерів) дорівнює q_M, доля чесних майнерів дорівнює q_H, причому $q_M + q_H = 1$ і $q_M < q_H$.

Зазначимо, що, згідно до процедури вибору слотлідерів, розподілу блоків у протоколі PoS між чесними слотлідерами та зловмисником підпорядковується біноміальному закону. Більш точно, це означає наступне: імовірність $P_{n,k}$ того, що у довільно вибраному відрізку з n послідовних таймслотів буде рівно k таймслотів, у яких слотлідером є зловмисник, дорівнює

$$P_{n,k} = C_n^k \cdot {p_M}^k \cdot {p_H}^{n-k}. \quad (1)$$

Твердження 1.

Нехай $l, n \in \mathrm{N}$, $l < n$. Тоді імовірність $P_{n,\geq l}^{(H)}$ того, що у ланцюжку з n послідовних таймслотів не менше за l таймслотів належать чесним стейкхолдерам, дорівнює

$$P_{n,\geq l}^{(H)} = \sum_{j=l}^{n} C_n^j \cdot {p_M}^{n-j} \cdot {p_H}^j. \quad (2)$$

Твердження 2.

Нехай $\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$. Тоді, якщо після виходу блоку $B*$ у мейнчейні минуло

$$n_{SP,TS}\left(\varepsilon_{SP}\right) = \arg\min_n \left(1 - P_{n,\geq z_{SP}\left(\varepsilon_{SP}^{(II)}\right)}^{(H)} < \varepsilon_{SP}^{(I)} \right) \quad (3)$$

таймслотів до відправки товару, то імовірність $P_{SP,DS}\left(n_{SP,TS}\left(\varepsilon_{SP}\right)\right)$ атаки подвійної витрати, яка відмінить цей блок, не перевищує ε_{SP}.

Твердження 3.

Визначимо подію $E_{SI} = E_{SI}\left(z_{SI}, n\right)$ як "за той час, як у сайдчейні вийшло z_{SI} блоків, у мейнчейні минуло менше за n таймслотів". Тоді

$$P\left(E_{SI}\right) \le 1 - e^{-\nu\cdot\tau\cdot n} \cdot \sum_{k=0}^{z_{SI}-1} \frac{\left(\nu\cdot\tau\cdot n\right)^k}{k!}. \quad (5)$$

3. Оцінка імовірності атаки подвійної витрати. Алгоритм визначення кількості блоків підтвердження (в залежності від заданої допустимої імов та параметрів мережі).

Виходячи з Тверджень 1-3, доведених у попередньому розділі, можна запропонувати наступний алгоритм визначення кількості блоків підтвердження у сайдчейні.

Алгоритм 1

Визначення кількості блоків підтвердження у сайдчейні, при яких імовірність атаки не перевищує задану величину

Вхід алгоритму:

параметри мейнчейну τ, p_M, p_H;

параметр сайдчейну ν;

допустима імовірність атаки ε.

1. Подати параметр ε як суму двох параметрів $\varepsilon = \varepsilon_{SP} + \varepsilon_{SI}$.

2. Подати параметр ε_{SP} як суму двох параметрів $\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$.

3. Використовуючи параметри мейнчейну, за формулою імовірності атаки з роботи [7], за заданим $\varepsilon_{SP}^{(II)}$ визначити таку (найменшу) кількість $z_{SP}\left(\varepsilon_{SP}^{(II)}\right)$ блоків підтвердження для мейнчейну, після якої імовірність атаки подвійної витрати у мейнчейні не перевищує задане $\varepsilon_{SP}^{(II)}$.

4. Використовуючи Твердження 1 і 2, та відповідні формули (2) та (3), визначити кількість таймслотів $n_{SP,TS}\left(\varepsilon_{SP}\right)$, за заданими значеннями $\varepsilon_{SP} = \varepsilon_{SP}^{(I)} + \varepsilon_{SP}^{(II)}$ та за значенням $z_{SP}\left(\varepsilon_{SP}^{(II)}\right)$, отриманим у пункті 3 цього Алгоритму.

5. За формулою (5) Твердження 3, визначити таку найменшу кількість блоків z_{SI} у сайдчейні, що величина $P\left(E_{SI}\right) < \varepsilon_{SI}$, тобто

$$z_{SI} = \arg\min_{z}\left\{1 - e^{-\nu\cdot\tau\cdot n} \cdot \sum_{k=0}^{z-1} \frac{\left(\nu\cdot\tau\cdot n_{SP,TS}\left(\varepsilon_{SP}\right)\right)^k}{k!} < \varepsilon_{SI}\right\}, \quad (9)$$

де величина $n_{SP,TS}\left(\varepsilon_{SP}\right)$ була обчислена у пункті 4 цього Алгоритму.

Вивід алгоритму: z_{SI}.

Теорема 1. Нехай величина z_{SI} отримана в результаті виконання Алгоритму 1 для заданих вхідних параметрів дворівневої мережі τ, p_M, p_H, ν та заданої величини ε. Тоді для імовірність $P\left(\tau, p_M, p_H, \nu\right)$ атаки

подвійної витрати на блок B_0 не перевищує ε, за умови що після виходу у мейнчейні відповідного блоку $B*$ у сайдчейні вийшло не менше за z_{SI} блоків.

Висновки.

У роботі отримані результати, які є необхідними для безпечного використання дворівневого блокчейну, згідно до протоколу Proof-of-Proof. Такий дворівневий блокчейн представляє найбільший інтерес для створення каскадної системи державних реєстрів, яка буде гарантовано захищена від підміни та підробки документів, а її користувачі – відповідно, від рейдерства. Крім цього, дворівневий блокчейн може використовуватись як середовище для смарт-контрактів, що має підвищену безпеку та таким чином спрощує юридичне обґрунтування статусу смарт-контракту.

Ми розглянули одну з чотирьох можливий комбінацій протоколів консенсусу, а саме – протокол консенсусу Proof-of-Stake в основному блокчейні (мейнчейні) та протокол Proof-of-Work в сайдчейні. Оскільки дві інші комбінації, коли в обох блокчейнах однакові протоколи консенсусу, були повністю досліджені у наших минулих роботах [5] та [6], то для подальшого дослідження залишається лише одна – Proof-of-Work в мейнчейні та Proof-of-Stake в сайдчейні.

1. Proof-of-Proof and VeriBlock Blockchain Protocol Consensus Algorithm and Economic Incentivization Specifications. (б. д.-b). Veriblock.org. https://veriblock.org/wp-content/uploads/2019/06/Proof-of-Proof_and_VeriBlock_Blockchain_Protocol_Consensus_Algorithm_and_Economic_Incentivization_v1.0.pdf
2. Saleh, F. (2021). Blockchain without Waste: Proof-of-Stake. Review of Financial Studies, 34(3), 1156–1190. https://academic.oup.com/rfs/article-abstract/34/3/1156/5868423
3. Nakamoto, S., (2008) A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf
4. Кондратенко, М. С. (2023). Використання технології блокчейну для побудови ієрархічної структури на множині державних реєстрів з метою захисту від підробки інформації. Електронне моделювання, 3(23), 43–56. https://www.emodel.org.ua/uk/archive-ukr/2023/45-3-u/c-43-56
5. Kovalchuk, L., Kostanda, V., Marukhnenko, O., & Pozhylenkov, O. (2022). Achieving Security in Proof-of-Proof Protocol with Non-Zero Synchronization Time. Mathematics, 10(14). https://www.mdpi.com/2227-7390/10/14/2422
6. Кондратенко, М. С. (2023). Визначення кількості блоків підтвердження у блокчейні, в якому розміщено реєстр другого рівня у випадку, коли в обох блокчейнах використовується протокол консенсусу POS. XLI Науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник матеріалів конференції, 188–190. https://ipme.kiev.ua/wp-content/uploads/2023/11/Матеріали_конференції_Survivability_and_Resilience-2023-4.pdf
7. Karpinski, M., Kovalchuk, L., Kochan, R., Rodinko, M., & Wieclaw, L. (2021). Blockchain technologies: Probability of double-spend attack on a proof-of-stake consensus. Sensors, 21(19). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8512294/

Л.В. Ковальчук, Н.В. Лисенко

ПЕРЕВАГИ ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ В ЕНЕРГЕТИЦІ ТА ПРОБЛЕМИ, ЯКІ ПОТРІБНО ВИРІШИТИ ДЛЯ ЇХ ВИКОРИСТАННЯ

Згідно загальноприйнятого визначення, **смарт-контракт** (англ. *smart contract* — «розумний контракт»):

- різновид угоди в формі закодованих математичних алгоритмів, укладення, зміна, виконання і розірвання яких можливі лише з використанням комп'ютерних програм (блокчейн платформ) в рамках мережі Інтернет;

- набір обіцянок у цифровому форматі, включно з протоколами, за якими сторони виконують ці обіцянки;

- комп'ютеризований протокол транзакцій, який виконує умови контракту [1];

- регулювання відносин сторін шляхом закріплення їх вираженої волі у формі певного коду, який придатний для зчитування комп'ютером.

Вважається, що вперше ідею смарт-контрактів висловиви Нік Сабо у 1996 р. [2], хоча незалежно від нього схожі ідеї також висловлювали також – Девід Чаум, Марк Міллєр. У своїх роботах він визначає смарт-контракт як «цифрове подання набору зобов’язань між сторонами, яке містить протокол виконання цих зобов’язань» та зазначає. що «нові інституції і нові способи формалізації відносин цих інституцій стали можливі» завдяки використанню смартконтрактів.

Не зважаючи на те, що смарт-контракти є дійсно зручним інструментом, вони на даний час не набули значного поширення на рівні державних органів – в першу чергу через те, що їх законодавчий статус не визначений. Так, єдиною країною, де смарт-контракти визнані законодавчо, є Білорусь (2016) [3].

Смартконтракти можуть існувати тільки всередині певного середовища, що має безперешкодний доступ виконуваного коду до об'єктів розумного контракту. Найбільш розповсюдженим середовищем існування смарт-контрактів є блокчейн. Смартконтракти на блокчейні – застосунок, середовищем існування якого є блокчейн. Вперше смарт-контракти були розроблені в блокчейні Ethereum (2013), співзасновником якого є засновник журналу Bitcoin Magazine Віталік Бутерін. Головна умова — дії повинні бути описані як математичні правила. [4]

Слід зазначити, що некоректно написаний смарт-контракт може завдати суттєвих збитків. Так, у червні 2016 року на мережу Ethereum була виконана атака, внаслідок якої з різних гаманців було виведено близько 50 млн USD.

Для програмування смарт-контрактів на даний час використовуються такі мови: Solidity (схожий на C або JavaScript); Vyper iSerpent (схожі на Python); LLL (низькорівнева версія Lisp); Mutan (заснований на Go) [5].

Ці мови дуже спрощені, але мають властивість повноти за Тьюрінгом. Це означає, що вони можуть реалізувати будь-яку логіку, яку можливо запрограмувати. В них є змінні, функції, умови, цикли, класи, наслідування.

Умови існування смартконтракту:

▪ можливість використання ЦП та асиметричного шифрування;

▪ існування відкритих, децентралізованих, доступних сторонам контракту баз даних, яким вони довіряють, для виконуваних транзакцій, робота яких повністю виключає людський фактор;

▪ децентралізація середовища виконання розумного контракту;

▪ правдивість джерела цифрових даних;

Зі смарт-контрактом пов'язані наступні об'єкти:

- підписанти — сторони смартконтракту, які погоджуються з умовами або відмовляються від умов контракту з використанням електронних підписів;

- предмет договору – об'єкт, що знаходиться всередині середовища існування розумного контракту, або ж повинен забезпечуватися безперешкодний, прямий доступ розумного контракту до предмету договору без участі людини;

- умови повинні мати повний математичний опис, який можливо запрограмувати в середовищі існування розумного контракту;

- децентралізована платформа**;**

- об'єкти розумного контракту.

Зі смарт-контрактом пов'язані як мінімум два відкритих ключі підпису: ключ того, хто створив контракт, та ключ самого контракту. Активувати смарт-контракт можна лише з особистого акаунта, але активований смарт-контракт в процесі виконання може звертатись до іншого смарт-контракту. Взагалі кажучи, змінити смарт-контракт, який вже розміщено у блокчейні, неможливо. Проте, за певних умов, його можна знищити і створити новий – лише в тому випадку, якщо в ньому є функція SELFDESTRUCT.

Основні властивості СК:

Розподіленість. СК відтворені та розподілені по всім нодам.

Детермінованість. Виконують дії, які в них записані, у відповідності до домовленостей, які в низ записані. Результат завжди прогнозований.

Автономність. Можуть автоматизувати всі види задач, працюючи як самовоконувана програма. Якщо СК не активізований, то він нічого не виконує. Не можна змінювати умови СК після його розробки.

Незмінність. Неможна змінити процес роботи СК після його розробки та активації, лише якщо він містить спеціальну функцію, через яку можна робити певні зміни.

Відсутність довіри. Сторони можуть взаємодіяти за допомогою СК навіть не знаючи один одного.

Прозорість. Код СК доступний розміщено у БЧ і він доступний всім.

Економність. Не потрібні витрати на «бюрократизацію».

Однією з **основних переваг** СК є можливість взаємодіяти в умовах повної недовіри і без посередників (невиконання умов анулює контракт).

Недоліки смартконтракту:

- можливі помилки – людський фактор (як було у ETH);
- невизначений юридичний статус (ускладнюється анонімністю, відсутністю посередників);
- не є універсальними; у певних випадках «класичні» договори зручніші;
- оплата за транзакцію, що містить/активує смартконтракт (газ).

СК на платформі блокчейн для розрахунків в електроенергетиці, у порівнянні з "класичними" контрактами, мають такі переваги:

- швидкі розрахунки за фактом споживання;
- зручний вибір трафіку;
- відсутність боржників;
- відмова від послуг посередників (зниження ціни за електроенергію на 5-10%).

Такі СК створюється за ініціативою однієї із сторін (споживач, мережа, генерація) і укладаються після погодження деталей.

Мета/очікування:

• зниження витрат при розрахунках за рахунок відмови від посередників;

• підвищення гнучкості пропозицій пи виборі тарифу та схеми оплати;

• підвищення ролі рядових споживачів у плануванні обсягів споживання;

• можливість закупок безпосередньо у виробників;

• захист учасників від навмисних маніпуляцій показниками засобів обліку;

• захист мережевих та генеруючи компаній від банкрутства компаній-продавців;

• захист споживачів від недостовірних даних стосовно відключень.

DTEK стосовно застосування смарт-контрактів:

В рамках комплексного підходу «3D» (Decarbonization, Decentralization, Digitalization), для укладання *P2P*-контрактів у галузі зеленої енергетики.

Очікування від введення смартконтрактів – дозволять використовувати p2p схему, що призведе до:

- спрощення многорівневої системи, що складається з виробників електроенергії, операторів розподільних мереж, операторів оптових розрахунків, трейдерів та споживачів.
- всі транзакції – через Інтернет;
- електроенергія стане дешевшою;
- за рахунок p2p, будуть мінімізовані втрати при передачі на великі відстані (зараз - 11%, як в бідних країнах; найнижчі – 2-3%, Тринідід і Тобаго, за рахунок відсутньої передачі на великі відстані).

Перша спроба використання p2p контрактів: Бруклін, 2016, продажа «зеленої» енергії сусіду.

За один рік різні компанії (LO3 Energy, Siemens, …) вклали у цю сферу більше за $ 300 млн.

Світові тренди P2P-технологій:

- форум BlockchainEnergyAsia в Сінгапурі;
- велика кількість азіатських блокчейн-проектів в енергетиці;
- P2P ринки електроенергії;
- в Японії запустили найбільший кластер розподілених систем накопичення енергії, що керується штучним інтелектом (більше 3500 домогосподарств), мета – розвантаження державної енергосистеми.

Проблеми на шляху розвитку P2P та СК у енергетиці:

• відсутність тенологічної бази у вигляді сонячних панелей, вітроустановок, накопичувачів енергії;

• невизначений правовий статус всієї криптоіндустрії;

• можливість реоргу блокчейну, при якому буде відмінено контракт, який вже почав виконуватись;

• можливість зупинки виконання контракту через брак коштів на його виконання.

Атаки на смарт-контракти та проблеми при виконанні:

- прихована вбудова зловмисних функцій, які можуть:

виконувати повторні транзакції з переведенням коштів;

виконувати будь-які непотрібні функції, за виконання яких даремно витрачається оплата, внаслідок чого контракт не відпрацьовує повністю;

- навмисне створення похибок в обчисленнях, що в результаті призводять до суттєвих відхилень;
- створення розгалуження у блокчейні, в результаті чого буде виконана лише частина зобов'язань по смарт-контракту;
- некоректне підключення до ресурсів (банківських карт, електромереж, тощо).

Шляхи вирішення проблем та запобігання атакам:

1. На перший час – створення простих типових смарт-контрактів, які будуть підтверджені і сертифіковані уповноваженим органом та матимуть документально підтверджений опис виконуємих функцій та послідовності їх виконання.
2. Для надійності – створення текстової копії смарт-контракту (що відповідає типовому смартконтракту), який теж підписується електронними підписами сторін, що укладають контракт.
3. Поступове ускладнення працюючих смарт-контрактів, шляхом додавання нових функцій, з повним документальним підтвердженням.
4. В деяких випадках – відкладене (до стабілізації блоку в блокчейні) виконання смарт-контрактів, в залежності від розрахункових значень кількості блоків підтвердження.
5. Використання чекпоінтів в блокчейні, у якому працює смарт-контракт.

6. Попередній (до початку виконання смарт-контракту) обрахунок витрат на його виконання і блокування цих коштів на початку роботи контракту (щоб гарантувати його повне виконання).

Приклад смарт-контракту в енергетиці:

вхід: кількість електроенергії, яку бажає закупити користувач;

- користувач знайомиться з контрактом та його підписує (активує);
- контракт запитує у користувача банківські реквізити та виконує відповідну автентифікацію (цей крок не виконується у випадку виконання попередньої автентифікації);
- контракт виконує розрахунок суми, яка включає в себе оплату за виконання контракту та за надання електроенергії, та блокує її на карті користувача;
- якщо коштів недостатньо, контракт видає попередження про це і зупиняється;
- якщо коштів достатньо, починає виконуватись, активуючи надання електроенергії;
- після надання вказаної кількості, гроші переводяться продавцю електроенергії, подача електроенергії припиняється;
- якщо електроенергія не була надана в повному обсязі, з технічних чи фізичних причин, то виконується перерахунок коштів, решта повертається на банківську карту.

1. Tapscott, Don; Tapscott, Alex (May 2016). *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World* (https://archive.org/details/blockch ainrevolu0000taps). с. 72 (https://archive.org/details/blockchainrevolu0000taps/page/72), 83, 101, 127. ISBN 978-0670069972.
2. Nick Szabo - Smart Contracts: Building Blocks for Digital Markets (https://web.archive.org/web/20180427165653/http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html). www.fon.hum.uva.nl. Архів оригіналу (http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html)
3. Беларусь первой в мире законодательно закрепила smart-контракт (https://www.belta.by/economics/view/belarus-pervoj-v-mire-zakonodatelno-zakrepila-smart-kontrakt-281784-2017/)
4. Создатель Ethereum Виталик Бутерин: «Блокчейн поможет искоренить коррупцию» (https://web.archive.org/web/20180220033328/https://incrussia.ru/blockchain/sozdatel-ethereum-vitalik-buterin-blokcheyn-pomozhet-iskorenit-korruptsiyu/). Архів оригіналу (https://incrussia.ru/blockchain/sozdatel-ethereum-vitalik-buterin-blokcheyn-pomozhet-iskorenit-korruptsiyu/) за 20 лютого 2018.
5. *Chris Dannen* ntroducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners.

О.В. Неласий, С.С. Самойлик, Г.В. Неласа

ПЛАТІЖНА СИСТЕМА ДЛЯ СТАНЦІЇ БЕЗДРОТОВОЇ ЗАРЯДКИ ЕЛЕКТРОКАРІВ З ВИКОРИСТАННЯМ СМАРТ-КОНТРАКТІВ

В останні роки спостерігається експоненційне зростання попиту на електромобілі (рис. 1). Хоча зростання ринків електромобілів у всьому світі ще не є глобальним явищем, цей тренд продовжує мати вирішальне значення з точки зору декарбонізації автомобільного транспорту, на який припадає приблизно одна шоста частина глобальних викидів. Якщо такий темп зростання збережеться, викиди CO_2 від автомобілів можна буде перевести у відповідність зі сценарієм чистих нульових викидів (NZE). до 2050 року [1]. Однак продажі часто сповільнюються через відносно високу закупівельну ціну електрокарів та відсутність зарядної інфраструктури в країнах.

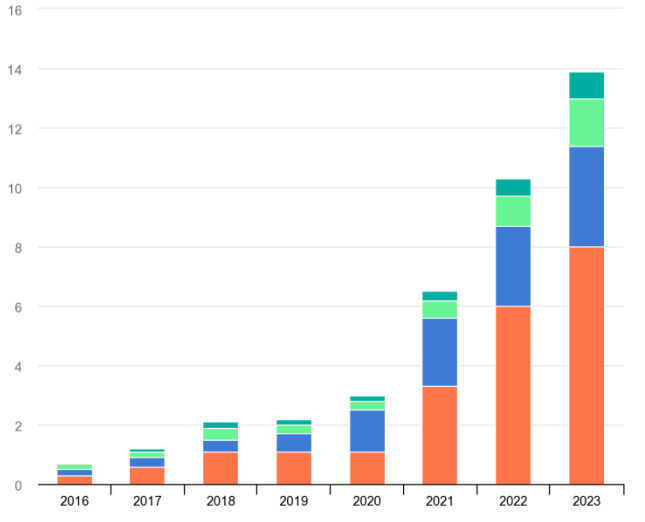

Рисунок 1 - Продажі електромобілів (млн.) [2]

Бездротова (безконтактна) зарядка електромобіля - це технологія, яка дозволяє заряджати електромобіль без необхідності фізичного підключення кабелю. Переваги бездротової зарядки включають зручність (не потрібно підключати кабель), безпеку та зниження несприятливого впливу погодних умов на заряджання. Проте цей метод також може мати деякі обмеження, такі як менша ефективність передачі енергії порівняно з проводовою зарядкою.

Методи безконтактної зарядки використовують принципи електромагнітної індукції та магнітного резонансу для передачі енергії. Резонансний зв'язок виникає, коли власні частоти двох систем — джерела та приймача мають дуже близькі значення.

Процес бездротової зарядки включає в себе встановлення зарядної платформи на поверхні (на приклад, на землі або на підлозі гаражу) і відповідного приймача на електромобілі.

Відомі стандарти бездротової зарядки [3] Qi, A4WP та PMA. Стандарт Qi працює на основі магнітної індукції. A4WP (Alliance for Wireless Power) позиціонується як технологія наступного покоління, що заснована на магнітному резонансі, та надає можливість заряджати кілька пристроїв одночасно. Стандарт PMA (Power Matters Alliance) також, як і Qi, має на увазі індуктивну зарядку, однак, іншу довжину хвилі.

Триває робота спеціалістів над специфікацією бездротової передачі електроенергії SAE J2954 [4], яка визначає прийнятні критерії сумісності, електромагнітної сумісності, мінімальної продуктивності, безпеки та тестування для бездротової передачі живлення для високопотужної бездротової зарядки транспортних засобів BEV і PHEV, для важких навантажень, бездоріжжя і застосування обладнання.

Компанія WiTricity[5] створює рішення для бездротової зарядки електромобілів. Розроблений для глобальної сумісності з галузевими стандартами, WiTricity Halo відповідає глобальним галузевим стандартам [6]: SAE, ISO, IEC і GB

Традиційно оплата за таку послугу здійснюється готівкою або банківською картою. В даній роботі досліджені особливості використання смарт-контрактів для автоматизації розрахунків клієнтів з постачальниками в подібних системах та проведено проектування архітектури програмного застосунку системи керування живленням передавачів бездротового заряду.

1. Electric Vehicles – Електронний ресурс – Режим доступу: https://www.iea.org/energy-system/transport/electric-vehicles
2. IEA, Electric car sales, 2016-2023, IEA, Paris https://www.iea.org/data-and-statistics/charts/electric-car-sales-2016-2023, IEA. Licence: CC BY 4.0
3. Не Qi єдиним! Розповідаємо про стандарти бездротової зарядки! – Електронний ресурс – Режим доступу: https://qinetiq.com.ua/https/www.qinetiq.com.ua/blogs/blog/first/
4. SAE TIR J2954 Wireless Power Transfer for Light-Duty Plug-In/ Electric Vehicles and Alignment Methodology – Електронний ресурс – Режим доступу: https://www.prweb.com/releases/sae_international_approves_tir_j2954_for_ph_ev_wireless_charging/prweb13421064.htm
5. WiTricity Halo™ Wireless Charging for Electric Vehicles – Електронний ресурс – Режим доступу: https://witricity.com/wp-content/uploads/2023/10/WiTricity-OEM-Brochure-Digital-1023.pdf
6. Commercialization & Global interoperability Standards– Електронний ресурс – Режим доступу: https://witricity.com/innovation/standards/

А.А. Макурін

ВИТРАТИ ЕЛЕКТРОЕНЕРГІЇ НА ВИДОБУТОК БІТКОЇНА ТА ТЕХНОЛОГІЯ БЛОКЧЕЙН

Визначення вартості видобутку, наприклад, одного біткоїну залежить від суми витрачених ресурсів. Наприклад, амортизація обладнання, що було використане для генерування нових блоків блокчейн, та щомісячні витрати на його обслуговування, вартість обслуговування швидкісного інтернету, налаштування програмного продукту майнінгу на певному пулі, сума витрат на електроенергію (дана стаття витрат є досить суттєвою і вимагає особливого контролю, в т. ч. проведення енергетичного аудиту, оскільки майнери часто намагаються зменшити витрати на електроенергію за рахунок її крадіжки), сума винагороди учасників майнінгу (оцінка даної статті витрат ускладнюється тим, що майнери отримують винагороду не лише під час процесу майнінгу, а й під час підтвердження операцій з переказу криптовалюти з одного гаманця на інший чи конвертації криптовалюти одну в іншу, при виводі її у фіатні гроші) тощо.

На рис. 1.1, 1.2 наведено результати дослідження Кембриджського університету, які засвідчують щорічне зростання споживання електроенергії при майнінгу біткоїну.

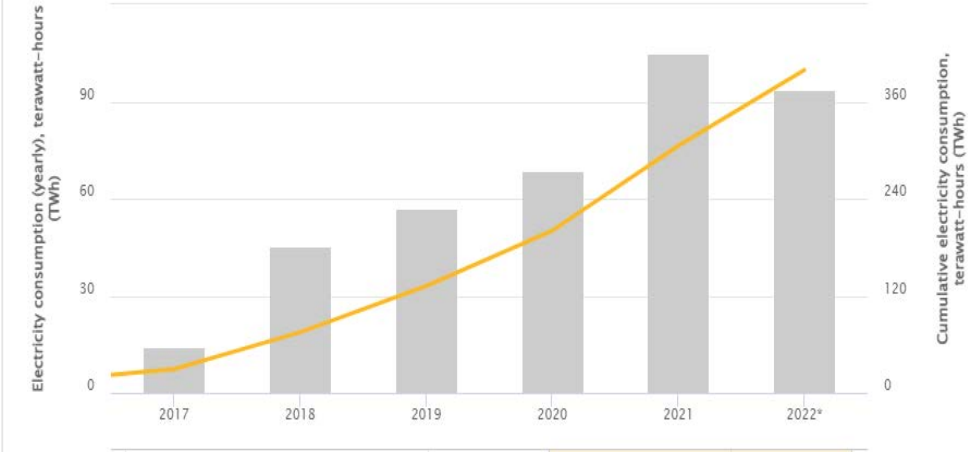

Рисунок 1.1. Загальне споживання електроенергії при майнінгу біткоїну протягом 2017–2021 рр. [1]

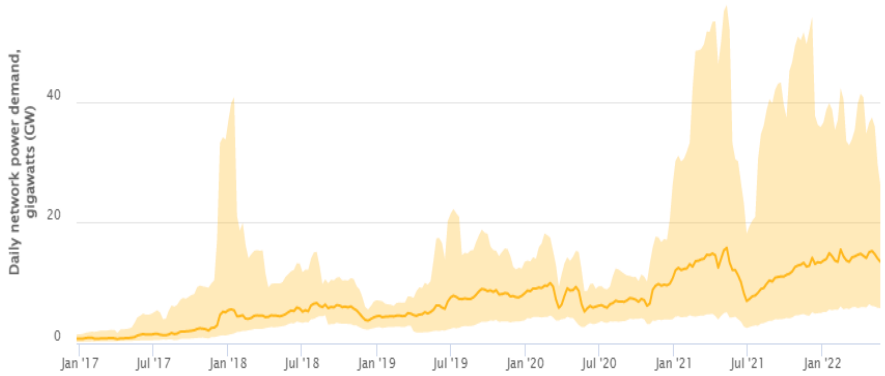

Рисунок 1.2. Щоденна потреба в електричних потужностях при майнінгу біткоїну протягом 2017–2021 рр. [2]

Як видно з рис. 1.2, в 2021 р. лише при виробництві біткоїну було витрачено близько 104,89 тВТ/год електроенергії, в той час як в 2020 р. – 68, 52 тВТ/год, що показує зростання споживання на 153 % протягом одного року, яке перевищує сукупне споживання електроенергії в таких країнах, як Пакистан та Філіппіни.

Застосування технології блокчейн також доцільне в сфері торгівлі електроенергією. Наприклад, оптові ринки енергії утворені зі складних процедур, які вимагають від сторонніх посередників, таких як брокери, торгові агенти, біржі, ціноутворювачі, транспортувальники, банки та регулюючі органи, узагальнити ключові аспекти транзакцій між усіма пов'язаними сторонами. Поточні процедури передбачають подальшу обробку вручну та посилення зв'язку для консолідації інформації, що зберігається окремо за кожною частиною транзакції. В результаті поточні процедури є повільними та тривалими, оскільки транзакції необхідно перевірити та узгодити кілька разів у період від початку до завершення, що призводить до зайвих витрат. Технології блокчейн та смартконтракти можуть дозволити створити агрегат для здійснення прямої торгівлі від постачальника до споживача енергії або роздрібної мережі через автономних торгових агентів, що виключають посередників. Агент шукав би найкращу пропозицію на ринку, аналізуючи прогнозований попит споживача на певний період.

Угода буде безпечно записана в блокчейн та автоматично виконуватися у визначений час системою самостійно. Виплати будуть відбуваються автоматично під час постачання, як зазначено в узгодженому договорі. Дані про транзакції будуть доступні всім сторонам та системному оператору через єдину точку доступу – блокчейн. Подібні перетворення вимагали б докорінних змін у нормативних актах.

Спочатку кількість транзакцій, які можна очистити за допомогою блокчейн часто на порядок менше, ніж це можливо за допомогою звичайних

електронних платежів, особливо тих, що використовують доказ алгоритмів роботи для досягнення консенсусу. Наприклад, мережа біткоїн, яка є найбільш розгалуженою серед криптовалют, що функціонує на основі блокчейн, може оновлювати та отримувати до 10 транзакцій в секунду, що можна запровадити в банківські операції – це значно підвищить запити з підтвердження та здійснення транзакцій, які обробляє банківська сфера.

Системи допуску (такі як Ethereum або Tendermint) можуть забезпечити потенційне розв'язання цього питання, однак впровадження таких рішень може бути значним при аналізі накладних витрат та вимагати ретельного проєктування та впровадження. По-друге, ми вважаємо, що теперішній структурі ринку енергоносіїв радикально змінитися за короткий проміжок часу буде складно. Тому багато чинних блокчейн проєктів, які зараз працюють, зазвичай зосереджені лише на одній частині всього енергетичного ринку, тобто ідентифіковані як найбільш легко піддані реалізації блокчейн, такі як врегулювання дисбалансу [3].

Blockchain значно допомагає з проведенням податкового контролю. Наприклад у КНР основною проблемою є оптимізація податкового законодавства та ухилення від сплати податків. Тому адміністрація країни видала доручення провайдеру інтернету послуг «Tencent» [3] зробити «розумний податок» на основі технології блокчейн для виявлення ухилень від податків.

Також у Флориді Відомство зі збору податків оголосило [4] про співпрацю з процесинговим сервісом BitPay для того, щоб почати приймати податки та збори за майно, водійські ліцензії, посвідчення особи, автомобільні номери та інші документи в криптовалютах Bitcoin та Bitcoin Cash [5].

Повертаючись до технології блокчейн варто зазначити, що в літературі наведено багато типів розподіленого алгоритму системи, кожен з яких має свої особливості, про що вже згадувалося раніше (Proof of Work; Proof of Stake; Practical Byzantine Fault Tolerance; Proof of Activity; Proof of Burn). Методологія, що використовується для досягнення консенсусу у мережах блокчейн, значною мірою визначає ключову продуктивність таких характеристик, як масштабованість, швидкість транзакції, безповоротність транзакцій, безпека та витрачання таких ресурсів, як електроенергія. В цілому, кожен метод вимагає процедури генерування і згодом – прийняття блоку. Блок можна створити або використати запропонований деяким вузлом у мережі, і він кодує ряд транзакції (наприклад, у криптовалютній системі – це грошові операції між різними рахунками). Наступний крок – досягнення консенсусу (прийняття запропонованого блоку з відповідних транзакцій всіма членами мережи). Як тільки блок прийнятий, він стає частиною блокчейн, а новостворені блоки – це криптографічно пов'язані з ним елементи. Через деякий час (залежно від консенсусу використовуваного алгоритму), блок стає постійною частиною блокчейн, тобто він стає остаточним (проте остаточність не виключає існування ймовірності того, що блок буде змінений чи спотворений, як частина майбутнього форку, що

виникає або за задумом, або в результаті кібератаки). Однак, ймовірність зміни зменшується з кожним новим доданим блоком, таким чином, створена блокчейн-система стає нескінченно довгою та стабільною.

1. Кембриджський біткоїн – індекс споживання електроенергії. Попит на потужність мережі Bitcoin. URL: https://ccaf.io/cbeci/index

2. Кембриджський біткоїн – індекс споживання електроенергії. Загальний обсяг виробництва та споживання. URL: https://ccaf.io/cbeci/index/comparisons

3. Tsaruk V. Ways to minimize the use of creative accounting practices in corporate structures. Innovative economy. 2020. № 1-2. P. 170-177.

4. Corbet S., Lucey B., Yarovaya L. Datestamping the Bitcoin and Ethereum bubbles . Finance Research Letters. 2018. Vol. 26. P. 81-88. URL : https://doi.org/10.1016/j.frl.2017.12.006.

5. IFRS Viewpoint Accounting for cryptocurrencies - the basics. Grant Thornton. 2018. 12 p. URL: https://www.grantthornton.global/globalassets/1.-member-firms/global/insights/article-pdfs/ifrs/ifrs-viewpoint-9---accounting-for-cryptocurrencies--the-basics.pdf

Н.О. Маслова, М.О. Рудською

ЕКСПЕРИМЕНТАЛЬНЕ СЕРЕДОВИЩЕ ДЛЯ ДОСЛІДЖЕННЯ ПРОГРАМНОГО КОНТЕНТУ

Вступ. Одним з поширених способів проведення деструктивних дій у відношенні інформаційних ресурсів є порушення захищеності програмного забезпечення комп'ютерних систем. Особливу увагу при цьому слід приділити безпеці комп'ютерних систем, які встановлені та застосовуються на об'єктах критичної інфраструктури. До критичних відносять комп'ютерні системи, які функціонують на об'єктах енергетики, водо- та теплопостачання, транспорту, державного управління. Згідно з [1] – це «об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам». Безпека критичної інфраструктури визначається таким станом захищеності, коли забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність й стійкість. А документ [2] визначає організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури.

Комп'ютерна система чи окрема програма, що встановлюється або експлуатується на об'єкті критичної інфраструктури, потребує дослідження, контроля та аналізу на всіх етапах життєвого циклу. Одним з методів контролю та дослідження програмного забезпечення є аналіз відповідності його контенту вимогам безпеки з застосуванням експериментального віртуального середовища (EVE). Підхід не є новим, він застосовується в експериментальних дослідженнях та тестуванні з метою зменшення навантаження на системи при проведенні складних експериментів, звільняє час і кошти експериментаторів, сприяє дослідженню небезпечних процесів [3]. EVE застосовується для підтримки нових програмних технологій, створенні й встановленні оновлених версій, контролі цілісності програмного забезпечення з тривалим терміном експлуатації.

Мета публікації опис експерименту зі розгортання й налаштування експериментального віртуального середовища для дослідження підозрілого контенту, перевірка працездатності створеного середовища.

Опис середовища. Шкідливе, уражене або підозріле програмне забезпечення (ПЗ), яке тим чи іншим чином потрапляє на комп'ютер користувача, може порушити функціонування, заблокувати роботу програмної чи апаратної частини критично важливої комп'ютерної системи, викрасти або спотворити важливі дані. Щоб унеможливити проникнення такого ПЗ в основну систему, створюється й налагоджується віртуальне тестове середовище. EVE - структура, яка блокує проникнення шкідливого контенту в основну систему, й без зупинки основного робочого процесу дозволяє провести детальне дослідження окремих програмних блоків, що

викликали підозру у впливі на функціонування базового програмного забезпечення [4].

Для розгортання експериментального віртуального середовища в даному випадку застосовувались наступні засоби:

- операційні системи Linux та Windows;
- програмне забезпечення віртуалізації (Ubuntu Linux та Windows VM);
- інструменти та пакети з середовища Python (ssdeep та pefile);
- система управління пакетами (pip);
- утиліта моделювання інтернет-служб (INetSim).
- Upx - пакувальник виконуваних файлів;
- бібліотеки YARA та YARA-Python (для виявлення, ідентифікації й класифікації шкідливого контенту);
- программа-анализатор Wireshark;
- консольна утиліта TShark (захоплення та аналіз мережевих пакетів);
- програма inetsim для налаштування Інтернет - зв'язку.

Основними характеристиками експериментального віртуального середовища слід наголосити:

- ізольованість;
- зручність;
- ефективність.

Ізольованість експериментального віртуального середовища означає, що програма, яка завантажена в експериментальному середовищі, не може впливати на роботу основної системи, надавати загроз пошкодження критично важливих програм або даних.

Зручність - це простота використання, зручний й звичайний АПІ, налаштування або запуск досліджуваного контенту в експериментальному середовищі повинен бути нескладним.

Ефективність - отримання очікуваного результату в максимально стиснуті терміни, відсутність впливу на продуктивність основної системи.

Опис експерименту. Віртуальна машина Windows – місце, де сумнівний контент виконується під час аналізу, а віртуальна машина Linux є ізольованою й використовується для моніторингу мережного режиму host-only. Якщо шкідлива програма буде вимагати DNS- сервіс, Linux VM надасть правильну відповідь DNS .

Створене віртуальне середовище було застосовано для проведення близько двадцяти експериментів. Шкідливий контент брався з сайтів: https://contagiodump.blogspot.com/; www.hybrid-analysis.com/; https://beta.virusbay.io/; https://avcaesar.malware.lu/; https://virusshare.com/; https://thezoo.morirt.com/; http://vxvault.net/ViriList.php.

У більш ніж шістдесяти відсотках випадків шкідливий контент було розпізнано й успішно видалено системними засобами віртуальних машин експериментального середовища. У двадцяти відсотках випадків шкідливе ПЗ розпізнати не вдалося. Результати експерименту наведено в Таблиці 2.

Таблиця 2 – Результати експерименту

Експеримент, №	випадків	% від кількості	Примітка
1,2,4,5,9,10,11,12,13, 17, 18	11	61,1%	виявлено
3, 8, 14, 16	4	22,2%	не виявлено
6,7,15	3	17,7%	інші ситуації

Під іншими ситуаціями маються на увазі випадки, коли в процесі виявлення та знешкодження підозрілого контенту сталося руйнування експериментального середовища. Що на думку авторів може свідчити про необхідність посилення захисту, встановлення додаткових антивірусних пакетів або підключення до баз аналізу відомих сигнатур вірусів.

Висновок. З метою забезпечення контролю захищеності програмного забезпечення критичних систем й перевірки підозрілого контенту сучасним підходом є застосування експериментального віртуального середовища. Без нього шкідливе, уражене програмне забезпечення чи потенційно небезпечні програми могли б отримати доступ до користувацьких даних та системних ресурсів. Застосування EVE надає можливості:

- проведення тестування оновлень програмного забезпечення перед їх встановленням;
- тестування роботи нових програм;
- перевірки сумнівних файлів;
- безпечного виконання підозрілого коду з метою унеможливлювання проявів шкідливого впливу на базову систему.

Результатом застосування EVE є:

- захищеність критично важливиз систем від прояв та дій підозрілого ПЗ;
- контроль оновлень програмних додатків, й впевненість у нормальному функціонуванню нових версій систем;
- виявлення прихованих експлойтів, шкідливих сігнатур та спроб атак що можуть бути вбудовані в програмне забезпечення;
- додатковий захист від певних штампів шкідливих програм, які, можливо, приховані в програмному забезпеченні.

Метою роботи було налаштування віртуальної машини для перевірки роботи підозрілого програмного контенту в їх середовищі. Під час роботи було налаштовано віртуальні машини, завантажено програми з підозрілим контентом, проведено аналіз результатів експерименту.

1. Закон України «Про критичну інфраструктуру», Документ 1882-IX, поточна редакція від 05.12.2022, чинний, https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури», із змінами, згідно з Постановою КМ № 991 від 02.09.2022, чинна, https://zakon.rada.gov.ua/laws/show/518-2019-п#Text
3. Experiments in Virtual Environments (EVE). https://cog.ethz.ch/the-lab/eve.html
4. Monnappa K A, Learning Malware Analysis: Packt Publishing Ltd., 2018. - 501p.

М.Л. Рафальський

СМАРТ-КОНТРАКТИ В СУЧАСНОМУ ПРАВОВОМУ ПОЛІ: АНАЛІЗ ЮРИДИЧНИХ ВРАЗЛИВОСТЕЙ ТА ВИКЛИКІВ

Сучасні технології, зокрема блокчейн, які забезпечують децентралізоване зберігання інформації, набувають особливої актуальності в галузі енергетики. Це стосується також смарт-контрактів, що вносять значний вклад у автоматизацію укладання договорів у цій сфері. Попри високий рівень захисту даних в децентралізованих системах, саме смарт-контракти можуть стати тою ланкою, через яку реалізуються цілеспрямовані атаки на блокчейн. У цій статті буде детально описано концепцію смарт-контрактів та їхні вразливості, які можуть призвести до правопорушень у таких децентралізованих мережах як блокчейн.

У рамках цієї теми розглянемо визначення віртуального активу за FATF (Financial Action Task Force on Money Laundering). Віртуальний актив - це електронне представлення вартості, яке можна обмінювати чи передавати у цифровому форматі, використовувати для платежів або як інвестицію. Також опираємося на Закон України «Про віртуальні активи», який на момент написання цього тексту ще не вступив у силу. Згідно із цим законом, віртуальний актив - це нематеріальне благо, що є об’єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. Існування та можливість обігу віртуального активу забезпечуються спеціальною системою. Такий актив може включати майнові права, зокрема право вимоги на інші об’єкти цивільних прав [1]. Щодо іншого аспекту, мас-медіа зазвичай вживають термін «криптовалюта» для позначення широкого спектру «криптоактивів» або «токенів». Ці токени можуть відображати різні типи фізичних чи цифрових товарів, включаючи цінні папери, колекційні предмети, гонорари, винагороди чи квитки на заходи. Термін «криптографічний актив» є більш універсальним і може бути застосований до певних видів токенів. Проте, слово «токен» є ще більш охоплюючим і стосується всіх типів токенів, не обмежуючись лише тими, що мають грошову вартість. Багато з цих нових активів не були створені з метою мати грошову вартість. Криптографічні токени використовуються для представлення програмованих активів або прав доступу, керованих смарт-контрактами та розподіленими реєстрами, як-от мережі блокчейн [2].

Блокчейн фактично являє собою спільну базу даних, що складається з записів, які потрібно підтвердити та зашифрувати. Всі блокчейни є прикладами розподілених реєстрів, проте не кожен розподілений реєстр є блокчейном. Хоча блокчейн виступає в ролі одного з видів розподіленого реєстру, він насправді становить лише частину таких систем [3]. Таким чином, технологія розподіленого реєстру представляє собою цифрову систему запису активних транзакцій, де транзакції та їхні деталі фіксуються одночасно в декількох місцях. Відрізняючись від традиційних баз даних,

розподілені реєстри не використовують єдине централізоване місце для зберігання даних чи центральні адміністративні функції [4]. Блокчейн є найбільш відомим видом розподілених реєстрів, який поділяється на публічні та приватні типи. Публічні блокчейни є відкритими мережами, доступними для будь-якої особи, що бажає долучитися до мережі, читати, писати або брати участь у процесах блокчейна. Ці блокчейни є децентралізованими без центрального органу управління, і дані у них неможливо змінити або модифікувати після перевірки. З іншого боку, приватні блокчейни контролюються адміністратором мережі, і учасникам потрібен дозвіл для приєднання. Вони керуються однією або декількома організаціями, що створює залежність від третіх сторін для проведення транзакцій. У цих блокчейнах лише сторони, що беруть участь у транзакції, обізнані про неї, тоді як інші учасники не мають доступу до цієї інформації, що робить транзакції приватними [5].

Наразі в Україні використання блокчейну є досить обмеженим і не широко розповсюдженим. Деякі державні установи, такі як ДП «СЕТАМ» та Держгеокадастр, вже використовують приватний блокчейн для операцій із нерухомістю, записуючи та відображаючи такі транзакції у реєстрі. Ми вважаємо, що із введенням в дію Закону України «Про віртуальні активи», кількість блокчейн-проектів, особливо в державному секторі, зокрема у сфері енергетики, збільшиться у відповідь на зростаючий попит на такі послуги.

Смарт-контракт — це цифровий протокол, створений за допомогою програмування. Його основна функція полягає у передачі інформації та забезпеченні дотримання умов, заданих у програмному коді, всіма сторонами. З юридичної точки зору, смарт-контракт можна описати як комп’ютерну програму, яка керує виконанням обов’язків між сторонами, що використовують його. Юридично, він може виконувати одну з двох ролей: безпосередньо реалізовувати умови, вбудовані в код, або моніторити дотримання або порушення умов, погоджених сторонами у контракті. Смарт-контракти дозволяють безпечно обмінюватися активами, такими як гроші, частки власності, цінні папери (особливо токенізовані) і інше, безпосередньо, без участі третіх сторін. Якщо сторонам потрібен довірений посередник, смарт-контракт може включити ескроу-агента. Він викладає умови зобов’язань у формі програмного коду, який виключає можливість різних трактувань або інтерпретацій. Це забезпечує однозначність виконання умов після узгодження та підписання контракту сторонами. Смарт-контракти виконуються автоматично, без потреби у втручанні людини [6].

Смарт-контракти фактично є програмами, заснованими на комп'ютерній логіці, які представлені у вигляді коду. Це дозволяє учасникам договорів бути впевненими в дотриманні всіх умов контракту, оскільки неможливо внести зміни або адаптувати їх на свій розсуд. В цьому контексті, код діє як фундаментальний закон для смарт-контрактів. Їх можна застосовувати у широкому спектрі фінансових операцій, включно із страхуванням, реєстрацією або передачею власності, кредитуванням та іншим. Особливо поширені смарт-контракти у бізнес-секторі, де вони використовуються для

організації виплат та дій, заснованих на платіжних дорученнях [7, с. 27]. Отже, смарт-контракт служить інструментом для автоматизації правових відносин. Проте, важливо врахувати, що така автоматизація має свої технічні та юридичні межі. При вирішенні питання про використання смарт-контракту, необхідно оцінити декілька "критеріїв придатності". Перший з них - це практичність і зрозумілість результатів. Автоматизувати варто ті правочини, що передбачають регулярні повторювані платежі або дії, а також угоди із великими сумами, де існує дефіцит довіри між сторонами та ризик невиконання фінансових зобов'язань. Другий критерій - технічна реалізація, тобто здатність інтегрувати умови угоди у програмний код смарт-контракту. Для цього умови повинні бути виражені через об'єктивні та кількісні параметри. Оптимальною моделлю для використання смарт-контрактів у юридичній практиці є "рікардіанський контракт" (Ricardian contract). Це метод, за яким угода фіксується у класичній юридичній формі з одночасним кодуванням її умов в інші системи, такі як розподілені реєстри або блокчейн. У випадку використання рікардіанського контракту, виконувані елементи тексту юридичної угоди подаються в форматі, який може бути представлений та реалізований як програмне забезпечення [6].

На даний момент в Україні відсутня можливість використання смарт-контрактів у правовій сфері через брак необхідного законодавчого регулювання. Проте, українське законодавство діє на засадах "що не заборонено, те дозволено", надаючи пріоритет свободі угод. Проблема застосування смарт-контрактів полягає в тому, що вони часто використовують криптовалюту, яка наразі не має офіційного правового статусу в країні. Що стосується відповідальності за порушення умов смарт-контракту, важливо врахувати відповідальність за умисні та необережні помилки. Вона може лягти на плечі сторін угоди, розробників смарт-контракту та інших третіх осіб. Одночасно, важливо пам'ятати, що відповідальність за помилки в смарт-контракті має брати на себе та сторона, яка взяла обов'язок його підготовки, та може залучати до цього розробників.

Втручання в роботу смарт-контрактів може відбуватися декількома шляхами:

Програмні помилки або уразливості. Найчастіше втручання в смарт-контракти відбувається через використання програмних помилок або уразливостей в коді. Це може включати баги, які дозволяють зловмисникам змінювати умови контракту або викрадати активи.

Зовнішні впливи та маніпуляції. Хакерські атаки або фішинг можуть бути спрямовані на користувачів смарт-контрактів, з метою отримання приватних ключів для доступу до контрактів.

Зміни в протоколі блокчейну. Іноді втручання може відбуватися через зміни в основному протоколі блокчейну, на якому базується смарт-контракт. Такі зміни можуть впливати на функціональність і безпеку контрактів.

Неналежне тестування. Недостатнє або неякісне тестування смарт-контракту перед його розгортанням може призвести до виявлення і використання уразливостей після запуску контракту.

Фронтраннінг атаки. Це вид атаки, при якій зловмисник використовує інформацію про майбутні транзакції у блокчейні, намагаючись виконати свою власну транзакцію перед ними, щоб отримати неправомірну вигоду.

Соціальна інженерія. Це методи, які використовуються для обману користувачів або адміністраторів смарт-контрактів, з метою змусити їх зробити щось, що дозволить зловмисникам втрутитися у роботу контракту.

Атака на програми-оракули. Необхідність зв'язку смарт-контрактів з реальним світом та отримання даних ззовні системи веде до використання так званих програм-оракулів. Ці програми-оракули — це спеціалізовані сервіси, які забезпечують інтеграцію цифрового та реального світу, надаючи смарт-контрактам необхідну інформацію для їхньої роботи. Залучення «оракулів» передбачає втручання третьої сторони в угоду, що вносить певні ризики. Основним питанням стає надійність даних, отриманих з таких джерел. Програми-оракули можуть бути вразливими до атак зловмисників, які можуть модифікувати їхній код, призводячи до поширення неправдивої або сфальсифікованої інформації. В результаті цього, дані, що надходять у смарт-контракт, можуть бути хибними, що призводить до несправедливого виконання угоди [8].

Для запобігання таким втручанням, важливо проводити ретельне тестування смарт-контрактів, регулярно оновлювати безпеку і слідкувати за останніми розробками в області криптографічної безпеки.

1. Про віртуальні активи [Інтернет]. Офіційний вебпортал парламенту України. [цит. за 18, Липень 2022]. Доступний у: https://zakon.rada.gov.ua/go/2074-20
2. What Is the Token Economy? - What Is the Token Economy? [Book] [Інтернет]. [цит. за 06, Вересень 2022]. Доступний у: https://www.oreilly.com/library/view/what-is-the/9781492072973/ch01.html
3. The Difference Between Blockchain and Distributed Ledger Technology [Інтернет]. Marco Polo Network. 2018 [цит. за 26, Липень 2022]. Доступний у: https://marcopolonetwork.com/distributed-ledger-technology/
4. distributed ledger technology (DLT) [Інтернет]. SearchCIO. [цит. за 26, Липень 2022]. Доступний у: https://www.techtarget.com/searchcio/definition/distributed-ledger
5. Difference between Public and Private blockchain [Інтернет]. GeeksforGeeks. 2020 [цит. за 27, Липень 2022]. Доступний у: https://www.geeksforgeeks.org/difference-between-public-and-private-blockchain/
6. Смарт-контракти: з чим вони смакують [Інтернет]. Блог Interlegal. 2018 [цит. за 07, Серпень 2022]. Доступний у: https://corporate.interlegal.com.ua/smart-kontrakti-z-chim-voni-smakuyut/
7. Озеракін М. Д. Розподілена система збереження даних на основі технології блокчейн : Магістерська дисертація. Київ, 2018. 134 с. Доступний у: https://ela.kpi.ua/bitstream/123456789/25554/1/Ozerakin_magistr.pdf
8. Юридична клініка НЮУ ім. Ярослава Мудрого Смарт-контракти та аспекти їх реалізації [Інтернет]. [цит. за 20, Березень 2023]. Доступний у: http://legalclinic.nlu.edu.ua/2023/01/26/smart-kontrakty-ta-aspekty-yih-realizacziyi/

С.А. Паршенніков, Л.В. Накашидзе

ГЕОТЕРМАЛЬНА ЕНЕРГІЯ: ВИКЛИКИ ТА ІННОВАЦІЇ

Геотермальна енергія, як важливий аспект сучасного енергетичного ландшафту, розглядається як стале джерело, що притаманно екологічній стійкості та відновлювальності. У контексті зростаючого питомого вагомості проблеми зниження викидів парникових газів, геотермальна енергія стає не лише ефективним, але й екологічно дружнім варіантом для задоволення енергетичних потреб людства. Визначаючи своєрідну стабільність у порівнянні з іншими джерелами енергії, геотермальна енергія викликає неабиякий інтерес науковців, інженерів та енергетиків, зокрема через її потенціал у суттєвому скороченні вуглецевого відбитку та сприянні збереженню навколишнього середовища[1].

Розглядаючи геотермальну енергію як потенційно значущий джерело в енергетичному спектрі, необхідно визначити серію складних проблем, що перешкоджають її повноцінному використанню. Першочерговим серед цих труднощів є географічні обмеження, які диктують нерівномірний розподіл геотермальних резервуарів по земній поверхні. Ці обмеження обумовлені не лише геологічними умовами, але й глибокими гідрогеологічними особливостями, що ускладнюють доступ до високопотенційних областей[1].

Додатковим важливим викликом є технічні труднощі, пов'язані з процесами буріння глибоких свердловин та подальшою експлуатацією геотермальних резервуарів. Забезпечення стійкості свердловин, оптимізація процесів тепловидобутку та вирішення технічних аспектів конверсії теплової енергії становлять значущі виклики для науковців та інженерів у цьому сегменті[2]. Розв'язання цих технічних завдань є необхідною передумовою для розширення геотермальної енергетики та підвищення її конкурентоспроможності у сучасному енергетичному пейзажі.

На шляху до вирішення складних викликів геотермальної енергетики, науковці та інженери зосереджують свою увагу на впровадженні інноваційних підходів. Однією з ключових областей інновацій є покращення технік буріння глибоких свердловин. Розробка високоефективних та стійких свердловин вимагає не лише високоточних інженерних рішень, але й використання передових матеріалів та технологій для забезпечення стійкості в умовах високих температур та тисків.

Додатково, інтенсивно ведуться дослідження та розробка технологій для низькотемпературних геотермальних резервуарів. Ця сфера інновацій спрямована на використання потенціалу тепловидобутку при менших температурних режимах, що розширює географічний охоплення геотермальними ресурсами та сприяє їх ефективнішому використанню[2]. Впровадження таких інновацій може значущим чином підвищити конкурентоспроможність геотермальної енергії та сприяти її більш широкому застосуванню у вирішенні енергетичних потреб суспільства.

В контексті розвитку геотермальної енергетики науковці та економісти звертають свою увагу на важливий аспект — аналіз ефективності та інвестиційні стимули, які визначають перспективи її інтеграції у сучасний енергетичний ландшафт. Передбачення та оцінка економічних вигід геотермальних проектів вимагає ретельного аналізу вартості виробництва, врахування експлуатаційних витрат та оцінки прибутковості на протязі тривалого періоду[2].

Інвестиційні стимули грають ключову роль у стимулюванні розвитку геотермальних технологій. Розробка ефективних фінансових механізмів та стимулів може значно полегшити відданість інвесторів у геотермальні проекти, зменшуючи фінансові ризики та роблячи ці проекти більш привабливими для потенційних учасників ринку[3]. При цьому важливо враховувати не лише фінансовий аспект, а й соціально-екологічні вигоди, що випливають зі зменшення викидів та створення нових робочих місць у регіонах розвитку геотермальних проектів.

В цілому, ретельний аналіз економічних параметрів та виважений підхід до стимулювання інвестицій в геотермальну енергетику визначають здатність цього джерела енергії виконувати стратегічну роль у досягненні енергетичної сталості та екологічної стійкості.

Розглядаючи геотермальну енергію як перспективний ресурс, неминуче виникає питання її впливу на місцеві спільноти та соціокультурні виклики, що можуть виникнути внаслідок впровадження геотермальних проектів[3]. Вплив на спільноти може бути подвійним: з одного боку, створення нових робочих місць та інфраструктури може сприяти соціально-економічному піднесенню місцевих громад, забезпечуючи їм нові можливості та ресурси.

Однак з іншого боку, геотермальні проекти можуть викликати соціокультурні виклики, пов'язані зі змінами в землекористуванні, традиційними способами життя та взаємовідносинами в спільнотах[4]. Важливо враховувати інтереси та думку місцевих мешканців у плануванні та реалізації геотермальних проектів, забезпечуючи їх участь та вигоди від енергетичних ініціатив.

Сприйняття геотермальних проектів у місцевих спільнотах також може залежати від ефективності комунікаційних стратегій та освітніх ініціатив, що мають на меті пояснення переваг та можливих викликів цих технологій[4]. Враховуючи соціокультурні аспекти, можна створити збалансований підхід до розвитку геотермальної енергетики, сприяючи взаємному розумінню та синергії між технологічними рішеннями та потребами суспільства.

У контексті розгляду геотермальної енергії як перспективного джерела електроенергії можна зробити висновок, що це технологічне рішення стає дієвим інструментом для досягнення енергетичної сталості та екологічної стійкості. Оцінка потенціалу геотермальних резервуарів, їхньої природної стійкості та низького вуглецевого відбитку свідчать про важливість подальших досліджень та інновацій у цьому секторі.

Розгляд проблем, зокрема географічних обмежень та технічних труднощів, підкреслює необхідність вдосконалення технологічних підходів,

зокрема у сфері буріння та оптимізації енергетичних процесів. Інновації в геотермальному секторі, такі як покращення буріння та використання низькотемпературних резервуарів, стають стратегічними напрямками для підвищення ефективності та географічного охоплення геотермальних проектів.

Аналіз економічних аспектів та інвестиційних стимулів свідчить про необхідність створення сприятливого фінансового середовища для привертання інвестицій та забезпечення сталого розвитку галузі. Одночасно, соціокультурні аспекти наголошують на важливості врахування інтересів та думки місцевих спільнот при впровадженні геотермальних технологій.

А також слід підкреслити необхідність подальших досліджень, спрямованих на вирішення ідентифікованих проблем та вдосконалення технологічних рішень. Розвиток геотермальної енергетики має потенціал відігравати вагому роль у забезпеченні сталої та надійної енергетичної системи, враховуючи виклики сучасного світу та сприяючи досягненню цілей сталого розвитку.

1. Барило А.А., Бенменні М. та інші, Відновлювальні джерела енергії: монографія/ ред. С.О. Кудрі, Київ: Інститут відновлювальної енергетики НАНУ, 2020. 392 с.
2. Буріння свердловин: бібліогр. покажч. уклад. Локотош Л. М.; ред. Жолобко Л. А. Івано-Франківськ: НТБ ІФНТУНГ, 2013. 46 с.
3. Федишин Б.П. Економіка енергетики. Навчальний посібник для студентів енергетичних спеціальностей вищих навчальних закладів. Тернопіль, 2003. 182 с.
4. Коробко Б. Енергетика та сталий розвиток: інформаційний посібник для українських ЗМІ. Київ. 2007. 40 с.

О.А. Пащенко, В.Л. Хоменко

ЮРИДИЧНІ ВИКЛИКИ ЗАСТОСУВАННЯ СМАРТ-КОНТРАКТІВ В ЕНЕРГЕТИЦІ

У світлі стрімкого технологічного розвитку, який охопив різні галузі сучасного суспільства, енергетичний сектор переживає неймовірні зміни та трансформації. Відчутна необхідність адаптації до вимог сучасності ставить перед енергетикою завдання не тільки підтримувати потреби суспільства у стабільному енергопостачанні, але й ефективно використовувати інноваційні технології для покращення управління та взаємодії.

Серед ключових інноваційних рішень, які визначають новий етап розвитку в енергетичній галузі, особливе місце займають смарт-контракти. Ці автоматизовані, децентралізовані та безпечні контрактні відносини визначають новий стандарт управління та взаємодії в стратегічно важливому секторі енергетики. Стаття, присвячена юридичним викликам та міжнародному досвіду використання смарт-контрактів укладання договорів у сфері енергетики, має на меті розкрити перспективи та труднощі впровадження цих інноваційних технологій. Висвітлення вказаних аспектів сприятиме не лише розумінню сучасного стану розвитку енергетичної сфери, а й визначенню оптимальних стратегій для подальшого просування у цьому динамічному середовищі.

Першим ключовим аспектом, який потребує ретельного розгляду, є визначення правового статусу смарт-контрактів. У контексті енергетичної сфери, де юридична чіткість є важливим елементом стабільності, необхідно визначити, як смарт-контракти взаємодіють з існуючим правовим середовищем. Розглядання цього аспекту дозволить з'ясувати, наскільки смарт-контракти можуть бути визнані та захищені в рамках чинного законодавства.

Другим важливим питанням є визнання юридичної обов'язковості смарт-контрактів. Враховуючи їхню автоматизовану природу, важливо з'ясувати, наскільки суди та правова система готові визнати зобов'язання, укладені через ці цифрові контракти. Порівняльний аналіз юридичної обов'язковості традиційних та смарт-контрактів стане основою для розуміння їхнього місця в юридичній системі.

Третім аспектом є проблеми, пов'язані з автоматизованою виконавчою владою смарт-контрактів. Якщо виникають спірні ситуації чи виникає необхідність виконання умов контракту, як саме смарт-контракти можуть забезпечити виконавчу владу та вирішення конфліктів? Це стає важливим елементом для більш глибокого розуміння практичної сторони використання смарт-контрактів в юридичному вимірі енергетичної індустрії.

Розглянемо детальніше що необхідно для визначення правового статусу смарт-контрактів є ключовим аспектом, який потребує ретельного розгляду в контексті їх використання в енергетичній сфері. Цей процес включає в себе

ряд аспектів та викликів, які впливають на юридичну обов'язковість та захист учасників контрактів.

Одним із важливих аспектів є визначення того, наскільки смарт-контракти можуть бути визнані юридичною сутністю. Автономність смарт-контрактів від традиційних юридичних рамок може створити виклики в їх визнанні, і тому важливо вивчати, як різні юрисдикції ставляться до цього питання.

Смарт-контракти повинні бути адаптовані до існуючого юридичного середовища енергетичної галузі. Це включає в себе врахування національних та міжнародних правових стандартів, щоб забезпечити їх взаємодію з існуючими юридичними нормами та правилами.

Важливо визначити, чи можна вважати смарт-контракти юридично зобов'язуючими угодами. Це стосується узгодження юридичного статусу смарт-контрактів з традиційними формами угод та їх визнанням перед судами.

Ще одним аспектом є забезпечення підтвердження волевиявлення сторін у смарт-контрактах. У відсутність фізичної форми підпису та паперового документа, важливо мати механізми для підтвердження згоди та наміру сторін у цифровому середовищі.

Суттєвим викликом є визнання електронного виконання умов смарт-контракту та його природи. Юридична система повинна визнати ефективність та дійсність виконання умов без необхідності традиційного підтвердження.

Узгодження цих аспектів є критичним для успішного впровадження смарт-контрактів у енергетичній галузі та визначення їхнього юридичного статусу. Це вимагає співпраці між технологічними та юридичними експертами для розробки ефективних регуляторних рамок, які враховують інноваційний характер цих цифрових контрактів.

Розглянемо питання визнання юридичної обов'язковості смарт-контрактів в енергетичній сфері, які потребують ретельного розгляду та вирішення ряду викликів.

Одним з ключових аспектів визнання юридичної обов'язковості смарт-контрактів є забезпечення їхньої прозорості та зрозумілості умов для всіх учасників. Зрозумілість тексту та логіки смарт-контракту є важливою для юридичної чіткості.

Для визнання юридичної обов'язковості смарт-контрактів важливо мати механізми підтвердження згоди сторін. Це може включати електронні підписи, двофакторну аутентифікацію чи інші методи для забезпечення дійсної волевиявлення учасників контракту.

Справедливе та ефективне вирішення суперечок є важливим елементом визнання юридичної обов'язковості. Якщо виникає потреба в судовому втручанні, система повинна бути готова визнати смарт-контракти та застосовувати до них судову владу.

Також важливим аспектом визнання обов'язковості є захист прав користувачів. Смарт-контракти повинні дотримуватися відповідних правових

стандартів та норм для захисту інтересів кожного учасника, зокрема енергетичних споживачів.

Визнання обов'язковості смарт-контрактів також вимагає порівняння з традиційними формами контрактів. Досягнення консенсусу щодо їхньої еквівалентності та прийняття цифрових контрактів в судовій практиці є важливим етапом.

Таким чином, врахування цих аспектів сприятиме визначенню механізмів та стандартів для визнання юридичної обов'язковості смарт-контрактів у сфері енергетики. Це важливий крок у напрямку розвитку ефективних та правовідповідних цифрових угод, що підтримають інновації в енергетичній індустрії.

Але автоматизована виконавча влада в смарт-контрактах також привносить свої власні виклики та аспекти, які потребують ретельного розгляду.

Однією з ключових проблем є забезпечення прозорості та ефективності виконавчих механізмів смарт-контрактів. Якщо виникає необхідність виконання умов контракту, система повинна чітко розуміти та автоматично виконувати визначені дії.

У випадку, коли ситуації викликають багаторазові суперечки, автоматизована виконавча влада повинна ефективно розв'язувати конфлікти та уникати надмірного виникнення юридичних проблем.

Для забезпечення правомірності виконавчих рішень, система повинна збирати та зберігати достатню кількість доказів виконання умов контракту. Це важливо для забезпечення справедливості та визнання результатів в судовій практиці.

З огляду на чутливість інформації, яка може включатися в смарт-контракти, існує проблема забезпечення конфіденційності та захисту особистих даних у контексті автоматизованої виконавчої влади.

В умовах, коли умови контракту можуть бути піддаються різним тлумаченням, автоматизована виконавча влада повинна бути здатна вирішувати ситуації невизначеності та запобігати можливим розбіжностям.

Важливим викликом є забезпечення синергії автоматизованих виконавчих механізмів смарт-контрактів з традиційними правовими та виконавчими процесами, щоб уникнути конфліктів та забезпечити гармонійне функціонування.

Визначення легітимного суб'єкта, відповідального за виконання смарт-контракту та вирішення спірних ситуацій, є важливим елементом для ефективності автоматизованої виконавчої влади.

Таким чином розгляд цих проблем допоможе зрозуміти, як можна покращити механізми виконавчої влади в смарт-контрактах, забезпечуючи їхню ефективність та відповідність в юридичному вимірі.

Таким чином можна зазначити що для використання смарт-контрактів в енергетичному секторі:

- необхідно визначити правовий статус смарт-контрактів у контексті енергетичного сектору, щоб забезпечити їхнє визнання та захист в рамках чинного законодавства;

- зробити порівняльний аналіз юридичної обов'язковості традиційних та смарт-контрактів що є ключовим для розуміння їхнього місця в юридичній системі;

- розв'язати проблеми, пов'язаних з автоматизованою виконавчою владою смарт-контрактів, що включає забезпечення прозорості, ефективності та розв'язання конфліктів.

Між тим міжнародний досвід підтверджує успішні впровадження смарт-контрактів в енергетичній галузі, а регуляторні ініціативи сприяють розвитку та стандартизації використання смарт-контрактів. Також треба звернути увагу на ефективні практики використання смарт-контрактів, які забезпечують ефективне управління енергетичними процесами.

Це забезпечить дослідження можливостей синергії смарт-контрактів з традиційними механізмами управління та виконавчою владою, розробку механізмів для забезпечення конфіденційності та захисту особистих даних у смарт-контрактах. Та подальше дослідження можливостей розширення юридичного визнання смарт-контрактів для забезпечення їхньої повноцінної інтеграції в правову систему.

1. Сегеда, І. В., Локотарев, Є. О., & Шаповал, В. О. (2019). Реалізація використання блокчейн-технологій у енергетичному секторі. Вчені записки Таврійського національного університету імені ВІ Вернадського. Серія: Економіка і управління, (30 (69),№ 4 (2)), 160-165.
2. Пащенко, О., Хоменко, В., & Коровяка, Є. (2023). Тенденції та перспективи використання цифрових технологій у навчанні.
3. Ніколаєв, С. О., Ковальов, Б. Л., Гриценко, П. В., & Одеволе, О. О. (2021). Блокчейн як фактор цифрової трансформації економіки України.
4. Азюковський, О., Павличенко, А., Пащенко, О., & Медведовська, Т. (2023). Базові інструменти та технології цифрової освіти. Grail of Science, (26), 386-389.

М.Ю. Родінко

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ПРОТОКОЛІВ КОНСЕНСУСУ BFT В ЕНЕРГЕТИЦІ

В останні роки технологія блокчейн набуває все більш широкого застосування у різних сферах. Не виключенням є і енергетичний сектор, де блокчейн може повністю змінити процес доставки енергоресурсів споживачів. Торгівля електроенергією чи фінансування енергетики можуть стати більш ефективними саме із залученням децентралізованих систем. Можливості використання блокчейн-технологій в енергетиці, зокрема, розглянуті в роботах [1,2].

Ключовою складовою системи, заснованої на технології блокчейн, є протокол консенсусу – механізм, що використовується для узгодження серед всіх вузлів в децентралізованій мережі. Серед криптовалютних платформ, на сьогодні найбільш відомими є два типи протоколів консенсусу: Proof-of-Work та Proof-of-Stake. Утім, застосування у блокчейні знайшли і BFT (Byzantine Fault Tolerance) протоколи, які часто використовуються у приватних мережах.

BFT є протоколом консенсусу, який забезпечує стабільну роботу мережі навіть при певній кількості зловмисних учасників (нод). Це досягається за рахунок механізму голосування між учасниками мережі. Якщо більшість учасників погоджуються з певним блоком, то цей блок додається до блокчейна.

У ході аналізу, було виявлено низку протоколів BFT, які мають досить різні властивості. Серед основних характеристик, які слід брати до уваги при оцінці протоколів BFT, можна виділити наступні:

- тип протоколу (детермінований / рандомізований);
- модель мережі (синхронна / частково синхронна / слабо синхронна / асинхронна);
- витрати (загальна кількість нод, необхідних для забезпечення безпеки);
- наявність лідера (на основі лідера / без лідера);
- продуктивність: пропускна здатність (кількість транзакцій або запитів в секунду) і затримка (час, необхідний для запуску протоколу);
- складність (кількість кроків; кількість повідомлень або бітів, що надсилаються одним вузлом);
- масштабованість.
- Різниця між різними типами мережевих моделей полягає в наступному:
- синхронний – всі повідомлення доставляються вчасно;
- частково синхронний – затримка Δ невідома протоколу;

- слабо синхронний – затримка Δ змінюється у часі, але поліноміально зростає за t;
- асинхронний – усі повідомлення зрештою доставляються.

Більшість існуючих протоколів BFT є слабо синхронними. Зауважимо, що властивості живучості слабко синхронних протоколів можуть повністю нівелюватись, якщо порушуються очікувані припущення щодо часу [3].

Таблиця 1 містить найвідоміші протоколи BFT, починаючи з найбільш ранніх і закінчуючи найсучаснішими та найпотужнішими протоколами BFT.

Таблиця 1 – Порівняння протоколів консенсусу BFT

Протокол	Рік	Кількість учасників	Модель мережі	Наявність лідера	Масштабо-ваність
Paxos [4]	1989	$3f + 1$	Слабо синхронна	Так	Ні
PBFT [5]	1999	$3f + 1$	Слабо синхронна	Так	Ні
Q/U [6]	2005	$5f + 1$	Асинхронна (живучість є слабкою)	Ні	Ні
HQ [7]	2006	$3f + 1$	Асинхронна (додаткові мови для живучості)	Ні	Ні
Zyzzyva [8]	2008	$3f + 1$	Слабо синхронна	Так	Ні
Aardvark [9]	2009	$3f + 1$	Слабо синхронна	Так	Ні
RBFT [10]	2013	$3f + 1$	Слабо синхронна	Так	Ні
hBFT [11]	2014	$3f + 1$	Слабо синхронна	Так	Ні
SCP [12]	2015	$3f + 1$	Частково синхронна	Так	Так
HoneyBudgerBFT [13]	2016	$3f + 1$	Асинхронна	Ні	Так
Elastico [14]	2016	$3f + 1$	Частково синхронна	Так	Так
Algorand [15]	2016	$3f + 1$	Слабо синхронна	Ні	Так
Hashgraph [16]	2016	$3f + 1$	Асинхронна	Ні	Так ($n \log n$)

Як видно з таблиці 1, майже для всіх протоколів загальна кількість нод становить $3f + 1$, де f – кількість зловмисних нод (це класична вимога BFT, але вона може змінюватися в деяких протоколах).

Усі ранні протоколи BFT були протоколами на основі лідера. У PBFT і пізніших протоколах лідер, який називається первинним, встановлює порядок запитів, зроблених усіма іншими вузлами (резервними). Деякі новітні масштабовані рішення припускають поділ на кілька комітетів, кожен з яких має свого власного лідера.

Більшість протоколів BFT погано масштабуються, багато з них можуть підтримувати лише до сотні вузлів.

Ми вважаємо, що протокол BFT, який було б доцільно використовувати в енергетичній сфері, повинен мати такі властивості:

- бути рандомізованим асинхронним протоколом;
- не мати лідера;
- мати хорошу пропускну здатність і масштабованість.

Два протоколи, які задовольняють описаним вимогам, це HoneyBudgerBFT і Hashgraph.

1. Chitchyan, R., & Murkin, J. (2018). Review of blockchain technology and its expectations: Case of the energy sector. *arXiv preprint arXiv:1803.03567*.
2. Bao, J., He, D., Luo, M., & Choo, K. K. R. (2020). A survey of blockchain applications in the energy sector. *IEEE Systems Journal*, *15*(3), 3370-3381.
3. The Intelligence of Information. The Honey Badger of BFT Protocols. URL: https://theintelligenceofinformation.wordpress.com/2017/02/22/asynchronous-bft-protocols-the-case-for-honey-badger/
4. Lamport, L. (2019). The part-time parliament. In Concurrency: the Works of Leslie Lamport (pp. 277-317).
5. Castro, M., & Liskov, B. (1999, February). Practical byzantine fault tolerance. In *OsDI* (Vol. 99, No. 1999, pp. 173-186).
6. Abd-El-Malek, M., Ganger, G. R., Goodson, G. R., Reiter, M. K., & Wylie, J. J. (2005). Fault-scalable Byzantine fault-tolerant services. *ACM SIGOPS Operating Systems Review*, *39*(5), 59-74.
7. Cowling, J., Myers, D., Liskov, B., Rodrigues, R., & Shrira, L. (2006, November). HQ replication: A hybrid quorum protocol for Byzantine fault tolerance. In *Proceedings of the 7th symposium on Operating systems design and implementation* (pp. 177-190).
8. Kotla, R., Alvisi, L., Dahlin, M., Clement, A., & Wong, E. (2007, October). Zyzzyva: speculative byzantine fault tolerance. In *Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles* (pp. 45-58).
9. Clement, A., Wong, E., Alvisi, L., Dahlin, M., & Marchetti, M. (2009). Making Byzantine fault tolerant systems tolerate Byzantine faults. In *Proceedings of the 6th USENIX symposium on Networked systems design and implementation*. The USENIX Association.

10. Aublin, P. L., Mokhtar, S. B., & Quéma, V. (2013, July). Rbft: Redundant byzantine fault tolerance. In *2013 IEEE 33rd international conference on distributed computing systems* (pp. 297-306). IEEE.
11. Duan, S., Peisert, S., & Levitt, K. N. (2014). hBFT: speculative Byzantine fault tolerance with minimum cost. *IEEE Transactions on Dependable and Secure Computing*, *12*(1), 58-70.
12. Luu, L., Narayanan, V., Baweja, K., Zheng, C., Gilbert, S., & Saxena, P. (2015). Scp: A computationally-scalable byzantine consensus protocol for blockchains. *Cryptology ePrint Archive*.
13. Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016, October). The honey badger of BFT protocols. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 31-42).
14. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 17-30).
15. Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017, October). Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th symposium on operating systems principles* (pp. 51-68).
16. Baird, L. (2016). Hashgraph consensus: fair, fast, byzantine fault tolerance. *Swirlds Tech Report, Tech. Rep.*

О.А. Сергієнко, П.О. Самусь

АНАЛІЗ ПОТОЧНОГО СТАНУ ПРАВОВОГО РЕГУЛЮВАННЯ ЦИФРОВИХ СМАРТ-КОНТРАКТІВ В УКРАЇНІ ТА В СВІТІ

Цифрові смарт-контракти є новим та перспективним феноменом, який має великий потенціал для розвитку цифрової економіки та суспільства. Вони мають ряд переваг перед традиційними договорами, таких як швидкість, ефективність, прозорість, безпека та зниження витрат. Однак вони також створюють нові правові виклики, пов'язані з визначенням їх правового статусу, відповідальністю сторін, захистом прав споживачів, врегулюванням спорів та іншими аспектами.

У 2020 році Україна посіла перше місце у світі за індексом адаптації блокчейну, який розробило аналітичне агентство Chainalysis[1]. З метою вдосконалення правового регулювання цифрових смарт-контрактів в Україні було розроблено та прийнято Верховною Радою України Закон "Про віртуальні активи" від 17.02.2022 р., який очікує на підписання Президентом [2]. Цей закон є першим в Україні, який визначає поняття віртуального активу, як "майнове право, що виникає на основі блокчейн-технології або іншої подібної технології, яке може бути об'єктом цивільних прав та обов'язків, а також може бути обмінене на інший віртуальний актив або фіатну валюту". Закон також встановлює правові засади регулювання віртуальних активів, їх емісії, обігу, зберігання, обміну, захисту та оподаткування.

Закон "Про віртуальні активи" також передбачає, що цифрові смарт-контракти можуть бути використані для укладання та виконання угод про віртуальні активи, якщо вони відповідають вимогам цивільного законодавства України. Закон також визначає, що цифрові смарт-контракти мають таку ж юридичну силу, як і традиційні договори, якщо вони відповідають вимогам цивільного законодавства України. Закон також надає право сторонам вибирати спосіб врегулювання спорів, що виникають з цифрових смарт-контрактів, або звертатися до суду.

Таким чином, Закон "Про віртуальні активи" є важливим кроком у правовому регулюванні цифрових смарт-контрактів в Україні, але він ще не вирішує всіх проблем, пов'язаних з цією сферою. Зокрема, закон не визначає поняття цифрового смарт-контракту, не враховує різні типи та класифікації цифрових смарт-контрактів, не встановлює правила щодо відповідальності сторін, захисту прав споживачів, стандартизації та інтероперабельності цифрових смарт-контрактів тощо. Тому потрібно подальше вдосконалення та розробка спеціальних нормативно-правових актів, які би враховували всі аспекти цифрових смарт-контрактів в Україні.

Правове регулювання цифрових смарт-контрактів є актуальною та невирішеною проблемою, яка потребує комплексного та гармонізованого підходу на національному та міжнародному рівнях. У різних країнах існують

різні моделі та ступені регулювання цифрових смарт-контрактів, які відображають їх специфіку, переваги та недоліки, схожості та відмінності. Можна виділити три основні моделі регулювання цифрових смарт-контрактів в світі: модель адаптації, модель модифікації та модель інновації. Кожна з них має свої переваги та недоліки, а також потребує подальшого вдосконалення та узгодження.

Модель адаптації. Ця модель передбачає, що існуюче законодавство про договори та електронні документи достатньо для визнання та захисту цифрових смарт-контрактів, а також для врегулювання спорів, пов'язаних з ними. Такий підхід мають багато країн Європейського Союзу, які базуються на Директиві про електронні договори від 08.06.2000 р., а також на Модельному законі про електронні договори Комісії ООН з міжнародного торговельного права (UNCITRAL) від 1996 р[3, 4]. Ця модель має перевагу в тому, що вона не потребує значних змін у законодавстві та не створює додаткових бар'єрів для використання цифрових смарт-контрактів. Однак вона має недолік в тому, що вона не враховує особливості цифрових смарт-контрактів, таких як їх автономність, незмінність, децентралізація тощо, а також не визначає їх правового статусу, відповідальність сторін, порядок врегулювання спорів тощо.

Модель модифікації. Ця модель передбачає, що існуюче законодавство про договори та електронні документи потребує доповнення та зміни для визнання та захисту цифрових смарт-контрактів, а також для врегулювання спорів, пов'язаних з ними. Такий підхід мають деякі країни, які прийняли окремі закони або поправки до існуючих законів, які визначають поняття, класифікацію, вимоги, права та обов'язки, відповідальність, порядок врегулювання спорів тощо щодо цифрових смарт-контрактів. Наприклад, такі закони прийняли штати Аризона, Невада, Теннессі, Вайомінг у США, а також Республіка Білорусь. Ця модель має перевагу в тому, що вона враховує особливості цифрових смарт-контрактів, а також визначає їх правовий статус, відповідальність, порядок врегулювання спорів тощо щодо цифрових смарт-контрактів. Однак вона має недолік в тому, що вона може створювати правову несумісність та нестабільність, оскільки різні країни та регіони можуть мати різні правила та стандарти щодо цифрових смарт-контрактів.

Модель інновації. Ця модель передбачає, що існуюче законодавство про договори та електронні документи не підходить для визнання та захисту цифрових смарт-контрактів, а також для врегулювання спорів, пов'язаних з ними. Такий підхід мають деякі країни, які прийняли нові та спеціальні закони, які створюють окрему правову категорію для цифрових смарт-контрактів, а також встановлюють нові правила та стандарти щодо їх використання та захисту. Наприклад, такі закони прийняли Мальта, Сінгапур, Естонія, Швейцарія тощо. Ця модель має перевагу в тому, що вона відповідає сучасним та майбутнім потребам та викликам цифрових смарт-контрактів, а також сприяє їх інноваційному розвитку та інтеграції. Однак вона має недолік в тому, що вона може бути надто радикальною та

експериментальною, а також може вимагати значних змін у суміжних галузях права, таких як цивільне, адміністративне, податкове тощо.

Для досягнення ефективного та збалансованого правового регулювання цифрових смарт-контрактів необхідно враховувати наступні фактори:

Визнання цифрових смарт-контрактів як договорів, які підпадають під дію загальних принципів та норм договірного права, але з урахуванням їх особливостей, таких як самовиконання, незмінність, децентралізація тощо.

Встановлення вимог до форми, змісту, укладання, виконання, розірвання, зміни та припинення цифрових смарт-контрактів, а також до прав та обов'язків, відповідальності, захисту прав та інтересів сторін, в тому числі споживачів.

Визначення порядку врегулювання суперечок, пов'язаних з цифровими смарт-контрактами, а також компетентних органів та процедур для їх вирішення, з урахуванням можливості застосування альтернативних механізмів, таких як медіація, арбітраж, онлайн-розмірковування тощо.

Гармонізація національного та міжнародного законодавства про цифрові смарт-контракти, а також співпраця та координація між різними країнами та регіонами, з метою створення єдиного та стабільного правового простору для цифрових смарт-контрактів.

Цифрові смарт-контракти є перспективним та викликаючим феноменом, який вимагає адекватного та своєчасного правового регулювання. Тільки за умови врахування їх переваг та недоліків, схожостей та відмінностей, а також забезпечення їх визнання та захисту, можна досягнути їх ефективного та безпечного використаня.

1. Chainalysis. (2020). The 2020 Geography of Cryptocurrency Report. https://go.chainalysis.com/rs/503-FAP-074/images/2020-Geography-of-Crypto.pdf
2. Закон України "Про віртуальні активи" від 17.02.2022 № 3637. https://zakon.rada.gov.ua/laws/show/2074-20
3. Директива 2000/31/ЄС Європейського Парламенту та Ради від 08.06.2000 р. про деякі аспекти електронної комерції в ринку внутрішніх послуг. https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX%3A32000L0031
4. UNCITRAL. (1996). Model Law on Electronic Commerce with Guide to Enactment 1996. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-09951_e_ebook.pdf

І.О. Усатий, О.М. Любименко, О.А. Штепа

ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ ДЛЯ КОНТРОЛЯ ЕНЕРГЕТИЧНИМИ ПОТОКАМИ В ЕНЕРГОСИСТЕМІ

За думкою фахівців, у найближчому майбутньому технологія блокчейн може істотно змінити енергетичну галузь та підвищити її ефективність. Наразі різні компанії та стартапи активно працюють над впровадженням новаторських децентралізованих рішень у цьому секторі, але через величезні обсяги ринку енергетики їхні зусилля ще не вистачають. Тому інвестиції в цьому напрямі вважаються досить обґрунтованими та привабливими. Забезпечення ефективного та надійного управління енергетичними потоками є важливим завданням для забезпечення стабільності та високої продуктивності енергосистеми.

В роботі розглядаються теоретичні та практичні аспекти використання блокчейн технологій для управління енергетичними потоками та методи їх оптимізації та аналізу впливу відновлюваних джерел енергії.

Дослідження включає в себе аналіз та моделювання роботи енергетичних систем з метою покращення їх продуктивності та стійкості, а також розробку рекомендацій для подальших досліджень у цій галузі. Важливість цієї теми полягає в забезпеченні сталості та ефективності енергетичних систем в умовах зростаючих вимог до енергоефективності та збереження критичної інфраструктури.

Аналіз останніх досліджень і публікацій у галузі використання блокчейн технологій для контроля енергетичними потоками в енергосистемі виявляє декілька ключових тенденцій та напрямків:

1. Розвиток методів оптимізації енергоефективності: Останні дослідження активно вивчають методи оптимізації виробництва, передачі та споживання електроенергії з метою підвищення ефективності використання ресурсів. Особлива увага приділяється використанню різних алгоритмів та технік оптимізації, включаючи машинне навчання, для забезпечення оптимального режиму роботи системи [1].

2. Вплив відновлюваних джерел енергії: З ростом використання відновлюваних джерел енергії, таких як сонячна та вітрова енергія, дослідження розглядають вплив цих джерел на управління енергетичними потоками. Акцент робиться на розробці алгоритмів та стратегій, які дозволять інтегрувати великі обсяги відновлюваної енергії в енергосистему та забезпечити стабільність роботи [2].

3. Використання нейронних мереж: Останнім часом спостерігається зростаючий інтерес до використання нейронних мереж для управління енергетичними потоками. Дослідження фокусуються на розробці нейромережевих моделей, які дозволяють передбачати та оптимізувати

роботу енергетичних систем, включаючи нормальний та аварійний режими [3].

4. Інтеграція розумних технологій: Розробка та дослідження методів управління енергетичними потоками також включає в себе інтеграцію розумних технологій та систем "розумних мереж" (Smart Grids). Це включає в себе використання сучасних засобів збору та аналізу даних для оптимізації розподілу електроенергії та підвищення стійкості системи [1].

Аналіз останніх досліджень та публікацій вказує на актуальність та значущість використання блокчейн технологій для контроля енергетичних потоків в енергосистемі та необхідність подальших досліджень у цій області.

В обраних методах дослідження враховувалася взаємодія між ними та різні аспекти управління енергетичними потоками. Застосування статистичних методів дозволило систематично аналізувати зібрані дані та встановлювати статистичні зв'язки між різними параметрами системи.

У роботі було проведено комплексний аналіз та дослідження проблеми управління енергоефективністю в сучасних енергетичних системах. Проведено системний аналіз даної тематики, де акцент був зроблений на актуальності та важливості завдань, пов'язаних із забезпеченням стабільності та оптимізації енергетичних потоків за допомогою техгнології блокчейн.

Ці дослідження вказали на те, що використання блокчейн технологій для контроля енергоефективності та оптимізації виробництва та споживання електроенергії є важливими завданнями в сучасних енергетичних системах. Тут також розглянута можливість використання методів машинного навчання, зокрема Q-навчання та нейронних мереж, для досягнення цих цілей.

В цілому в дослідницькій роботі наведено детальний огляд сучасних досліджень з використанням блокчейн технологій для контроля та розробок методів управління енергетичними потоками в енергосистемах. Вони охоплюють аналіз різних підходів до управління енергетичними потоками, використання аналітичних методів, вплив відновлюваних джерел енергії та необхідність розробки інформаційних систем для управління енергетичними потоками. Цей підхід сприяв створенню комплексного підходу до вирішення поставлених завдань та забезпечив високу достовірність отриманих результатів та висновків, що є важливим для подальшого розвитку використання блокчейн технологій в області управління енергетичними потоками в енергосистемі.

1. Sutton, R. S., & Barto, A. G. (2018). "Reinforcement Learning: An Introduction." MIT press.
2. Zhang, N., Sun, H., Chen, Z., & Luh, P. B. (2014). Optimization models for integrated energy systems in smart grid with renewables. IEEE Transactions on Smart Grid, 5(5), 2474-2483
3. "Deep Learning for Time Series Forecasting: Predicting Sunspots with Keras" (Jason Brownlee, 2018).

Д.О. Феденко

БЛОКЧЕЙН ТЕХНОЛОГІЇ В ЕНЕРГЕТИЦІ: СИНЕРГЕТИКА ТА ПРАКТИКА

У сучасному світі, де відбувається стрімкий розвиток технологій, блокчейн виходить за межі фінансового сектору та знаходить своє втілення в різних галузях, включаючи енергетику. Використання блокчейн технологій у сфері енергетики відкриває нові можливості для оптимізації процесів, забезпечення безпеки та створення більш демократичного енергетичного ландшафту.

1. Синергетика блокчейну та енергетики:

Блокчейн в енергетичній галузі дозволяє створити синергію між різними учасниками системи – виробниками, споживачами та дистриб'юторами енергії. Створюючи розподілену систему обліку, блокчейн дозволяє взаємодіяти сторонам без посередників, що сприяє оптимізації процесів та зниженню витрат.

2. Децентралізована виробництво та обмін енергією:

Блокчейн дозволяє виробникам енергії, таким як власники сонячних панелей чи вітрових установок, безпосередньо обмінювати вироблену енергію з іншими учасниками системи. Це створює більш ефективну та сталу модель виробництва та споживання енергії.

3. Системи "Розумного грида":

Блокчейн може бути використаний для створення "розумних грідів" – інтелектуальних мереж, які автоматично регулюють виробництво та розподіл енергії з урахуванням поточних потреб і ресурсів.

4. Боротьба з енергетичними втратами:

Децентралізовані системи на базі блокчейн технологій дозволяють уникнути значної частини енергетичних втрат, що виникають при транспортуванні енергії на великі відстані, оскільки виробники можуть забезпечувати споживачів на місці виробництва.

Блокчейн технології в контексті енергетики створюють синергію, що дозволяє покращити ефективність та демократизувати виробництво та споживання енергії. Основна ідея полягає в тому, щоб створити децентралізовану мережу, де різні учасники можуть взаємодіяти напряму, обходячи традиційних посередників.

- **Міжвиробничий обмін енергією:** Блокчейн дозволяє виробникам енергії (наприклад, власникам сонячних панелей чи вітрових установок) безпосередньо обмінювати свою вироблену енергію з іншими учасниками мережі. Це може відбуватися через "розумний контракт" в блокчейні, який автоматично фіксує та виконує умови угоди. Такий підхід сприяє виникненню місцевих, децентралізованих енергетичних систем.

- **Ефективніше використання ресурсів:** Блокчейн може допомагати оптимізувати використання ресурсів, таких як енергія, шляхом створення "розумних грідів". Ці інтелектуальні системи можуть автоматично регулювати виробництво та розподіл енергії в режимі реального часу, враховуючи попит та змінність виробництва з відновлювальних джерел.
- **Безпека та довіра:** Технологія блокчейн забезпечує високий рівень безпеки та довіри в області енергетики. Кожна транзакція фіксується в блокчейні, і ця інформація невідредагована. Це дозволяє підвищити рівень впевненості між учасниками системи та зменшити ризики маніпуляцій чи обману.
- **Підтримка новаторських бізнес-моделей:** Блокчейн відкриває двері для нових бізнес-моделей в енергетиці. Власники відновлювальних джерел енергії можуть, наприклад, отримувати компенсацію за надлишкову енергію, яку вони виробляють і подають у мережу.
- **Зменшення залежності від посередників:** Традиційна модель енергетичного ринку часто передбачає багато посередників, що додає витрат та складність процесів. Завдяки блокчейну, можливе створення прозорих та ефективних систем, де взаємодія відбувається напряму між учасниками, зменшуючи роль посередників.

1. 1.Brooklyn Microgrid [Електронний ресурс]. – Режим доступу: http://brooklynmicrogrid.com/.
2. Urszula Papajak. Can the Brooklyn Microgrid project revolutionize the energy marke? / Urszula Papajak // Medium (Nov. 2017) [Електронний ресурс]. – Режим доступу: https://medium.com/thebeammagazine/canthe-brooklyn-microgrid-projectrevolutionise-the-energy-marketae2c13ec0341.

Чемерис О.А.

ІНФОРМАЦІЙНІ СИСТЕМИ ЕНЕРГЕТИКИ, ПОБУДОВАНІ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Розвиток сучасної енергетики проходить відповідно концепції 3D – Декарбонізація, Децентралізація, Діджиталізація [1]. В цей процес технологія блокчейн вкладає великий потенціал створення та розвитку безпечних та захищених від зовнішнього втручання інформаційних систем, спрямованих на вирішення різного роду задач енергетики. . Інформаційно-комунікаційні технології останнім часом почали революціонізувати енергетичний ландшафт, а тепер технологія блокчейн надає додаткову можливість зробити енергетичну систему більш розумною, ефективною, прозорою та безпечною у довгостроковій перспективі [2].

Blockchain технології можуть бути застосовані в різних процесах, пов'язаних з операціями та бізнес-активністю енергетичних компаній [3]. Застосування та перспективи використання, які можуть бути використані при побудові інформаційних систем енергетики, наведено далі:

Біллінг: блокчейн, розумні контракти та розумне вимірювання можуть реалізувати автоматизовану систему розрахунків для споживачів та розподілених генераторів електроенергії. Комунальні компанії можуть скористатися потенціалом для мікро-платежів за енергію, програмних рішень платіжних платформ для оплати відповідно за лічильниками.

Продажі та маркетинг: практика продажів може змінюватися відповідно до енергетичного профілю споживачів, індивідуальних переваг та екологічних проблем. Блокчейн, в поєднанні зі технологіями штучного інтелекту, такими як, наприклад, машинне навчання, можуть ідентифікувати споживачів електроенергії і, отже, забезпечити індивідуальне надання енергетичного забезпечення з доданою вартістю.

Торгівля та ринки: форми розподіленої торгівлі з блокчейном є перспективні для ринкових операцій, таких як управління оптовим ринком, операції з торгівлі та управління ризиками. Системи з використанням блокчейн технологій в даний час розробляються також для торгівлі зеленими сертифікатами [4].

Автоматизація: Блокчейн може покращити управління децентралізованими енергетичними системами та мікромережами [5]. Впровадження локальних ринків енергії, що що побудовані на основі блокчейн технологій з організацією торгівлі енергією на однорангових мережах (P2P маркет), або розподіленими платформами, може значно збільшити виробництво енергії та локальне споживання, що потенційно може позитивно вплинути на доходи та тарифи.

Смарт-грід і передача даних: Blockchain потенційно може бути використаний для зв'язку смарт-пристроїв, передачі даних або зберігання. Інтелектуальні пристрої в інтелектуальній енергосистемі включають

інтелектуальні лічильники, розширені датчики, обладнання для моніторингу мережі, системи управління та управління енергією, а також розумні домашні контролери енергії та системи моніторингу будівель.

Незважаючи на серйозний потенціал, який демонструє Blockchain, застосування цієї технології має свої обмеження.

Надлишковість інформації. Blockchain створює кілька копій баз даних на кожному вузлі в мережі. Це необхідно для роботи самої технології і для безпеки. Однак багаторазове копіювання інформації створює надмірність. Відповідно, в транзакції беруть участь всі вузли мережі. Це необхідно для роботи консенсусних алгоритмів. Все це призводить до необхідності мати достатню кількість пам'яті на кожному вузлі для зберігання інформації про всі транзакції, не кажучи вже про значне споживання енергії в процесі написання. Тому застосування Blockchain в майбутньому вимагає вирішення питань надмірності.

Продуктивність і масштабованість. Як система для операцій P2P Blockchain, швидкість обробки транзакцій набагато нижча, ніж її централізований аналог. На відміну від інших розподілених систем, додавання нових вузлів в Blockchain не підвищує його продуктивність. Більш того, залежно від застосовуваного консенсусного протоколу швидкість обробки транзакцій може знижуватися зі збільшенням учасників. Розробляються інші консенсусні протоколи для вирішення цих проблем.

Безпека смарт-контракту. Смарт контракт - це програма, написана людиною. Відповідно, можуть бути помилки і уразливості. У програмних компаніях такі проблеми вирішуються шляхом випуску нових версій з помилками. Однак сама природа Blockchain не дозволяє вносити зміни в існуючі контракти. Для вирішення цих питань необхідно розробити механізми виявлення вразливостей до укладення контракту в Blockchain.

Взаємодія Blockchain. Адаптація Blockchain до майбутніх енергосистем, включаючи взаємодію з IoT, потребує значних зусиль. Хмарні системи мають обмежену пропускну здатність. Blockchain консенсус протоколи виробляють значні обсяги трафіку. Тому необхідні подальші поліпшення. Більш того, впровадження технології Blockchain вимагає узгодження з усіма гравцями енергетичного ринку, що є нетривіальним завданням.

Впровадження Blockchain у фізичну енергетичну структуру. На рівні кібер-інформації Blockchain і смарт-контракт забезпечують безпеку. Однак зміни в розташуванні генератора і споживача, які відбудуться при укладенні договору, вплинуть на потік енергії у фізичному світі (розгін мережі), що може призвести до таких проблем, як перевантаження мережі, відхилення напруги і т.д. Тим не менш, рішення цих проблем розробляються.

Це тільки приклади обмежень. Технологія блокчейн має вразливості, пов’язяні зі зловмисними діями, або зовнішнім втручанням в роботу системи. До таких дій відносяться: атака 51%; крадіжка або втрата ключової пари, програмні уразливості; аналіз дій користувача; атака затемнення (Eclipse); двохкратна витрата; егоїстичний майнінг (Selfish Mining), тощо. Вирішенню цих проблем мають бути присвячені майбутні дослідження.

1. Кириленко О.В. Заходи та засоби перетворення енергетики України на інтелектуальну екологічно безпечну систему. ISSN 1027-3239. Вісн. НАН України, 2022, № 3, doi: https://doi.org/10.15407/visn2022.03.018

2. Khatoon, A.; Verma, P.; Southernwood, J.; Massey, B.; Corcoran, P. Blockchain in Energy Efficiency: Potential Applications and Benefits. Energies 2019, 12, 3317. https://doi.org/10.3390/en12173317.

3. L. Ali, M. I. Azim, J. Peters, N.B. Ojha, V. Bhandari, A. Menon, V. Tiwari, J. Green, S.M. Muyeen, and M.G. Simoes P2P Trading-enabled Local Energy Market Supplemented with Blockchain Technology: An Australian Case Study, 2023, IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 2023, pp. 51-55, doi: 10.1109/GreenTech56823.2023.10173850

4. Indigo Advisory Group. Blockchain in energy and utilities use cases, vendor activity, market analysis, ⟨https://www.indigoadvisorygroup.com/blockchain⟩, 2017.

5. Чемерис О.А. Задачі технології блокчейн для електричних мікромереж. Проблеми інформатизації та управління, 1(61)’2019. с. 102-107.

В.О. Шведов, Ю.І. Рудик, В.Р. Куць

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОЄКТІВ БЛОКЧЕЙН-ГРІД ЕЛЕКТРОПОСТАЧАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Бурхливий розвиток відновлювальної енергетики приводить до істотного збільшення її частки у виробленні електроенергії, тому питання інтеграції нестабільних джерел енергії в мережу без послаблення надійності системи стоїть на порядку денному в багатьох країнах. Крім збільшення частки відновлюваної енергії в національному енергобалансі, нестабільність попиту і пропозиції енергії посилюється розвитком розподіленої генерації те електрифікацією легкового транспорту. Україна не може ігнорувати факт світові зміни технологічної моделі в електроенергетиці і пов'язані з цим виклики і зрушення в розвитку галузі. В іншому випадку країна зіткнеться з низкою ризиків. Перший з них - ризик отримати дорожчу і менш гнучку електроенергетику в порівнянні з іншими індустріально розвиненими країнами, позбутися ряду нових ринків та істотно обмежити розвиток нової (цифровий) індустрії. [1-3].

Блокчейн - розподілена база даних, яка зберігає інформацію про всі транзакції учасників системи у вигляді «ланцюгів блоків» (англ Blockchain). Доступ до реєстру є у всіх користувачів блоку, які виступають як колективні нотаріуси, що підтверджує істинність інформації в базі даних. Інакше кажучи, це ніби децентралізована (розміщена у всіх його користувачів одночасно) цифрова «книга обліку», у якій фіксуються всі операції й зберігається різноманітна інформація. Блокчейн має значний потенціал трансформувати співпрацю і взаємодію компаній для прискорення розвитку низьковуглецевої енергетики. Зокрема, його механізми можуть застосовуватися, починаючи з відстеження відновлювальних джерел енергії – і до зміни співвідношення типів виробництва й споживання енергії. Блокчейн може відіграти ключову роль у створенні прозорої, більш стійкої й ефективної низьковуглецевої енергетичної системи у світових масштабах. У державі, яка являє собою сукупність енергонезалежних міст-островів, мегаполісів які сформовані із хмарочосів, які самостійно забезпечують себе енергією, або купують надлишок виробництва сусіднього хмарочосу за смарт-контрактами, які функціонують на блокчейн-платформах [4], побудованих на використанні інтелектуальних технологій управління, показав визначені переваги робастних систем для управління електропостачанням і в кризових ситуаціях для об'єктів критичної інфраструктури. Попередніми дослідженнями була проведена оцінка позитивної можливості застосування таких систем для конкретного технологічного комплексу і запропонована структура інтелектуальної системи управління процесом буріння нафтових і газових свердловин із можливістю зниження впливу форс-мажорних обставин. Прийнявши за

основу такий аналіз та схожі приклади керування і стійкості закордонних об'єктів «наногрід» та «мікрогрід» можна буде зробити висновки про адаптивність та необхідну маневреність ресурсів для вітчизняної енергосистеми або елементів «смартгрід», як частини електричних мереж.

На основі [5-9] зрозуміло основні види енергетичних рішень, що Одним із можливих напрямів застосування блокчейну є так званий «Інтернет енергії» - тип децентралізованої електроенергетичної системи, в якій реалізовано інтелектуальне розподілене управління, здійснюване за рахунок енергетичних трансакцій між її користувачами. «Інтернет енергії» - відповідно до дослідження Navigant research «Transactive Energy Markets», який опубліковано у 2018 році - це peer-to-peer електроенергетика, в якій взаємодія між виробниками і споживачами електроенергії, торгівля електроенергією і різними послугами, а також режимне управління енергосистемою здійснюються за рахунок прямих трансакцій між користувачами. Простіше кажучи, енергосистема стає мультивекторна, всі учасники енергетичного ринку матимуть багато функцій, таких як постачання електричної енергії, участь в режимному управлінні та підтримці частоти і рівня напруги, надання енергетичного обладнання в «віртуальну» оренду, забезпечення резерву потужності і будь-які інші види послуг, які можуть бути надані в електроенергетиці.

Застосування інструменту підвищення національної стійкості має два джерела гнучкості: розподілені джерела енергії та управління попитом на електроенергію. Англійська мережевий оператор Ofgem визначає гнучкість як здатність до зміни патернів (режимів) виробництва і споживання енергії у відповідь на зовнішні, як правило, цінові сигнали для надання системних послуг. Прикладом є проект, що реалізується міжнародним технологічним консорціумом, який представляють:

- торговий дім ITOCHU, що здійснює виробництво та продаж накопичувачів Smart Star,
- збутова компанія TRENDE, продає електроенергію домогосподарствам за спеціальним тарифом, стимулюючого використання накопичувачів для розвантаження енергосистеми,
- NF Corp. надає IoT-платформу для віддаленого доступу до накопичувачів,
- нарешті, MOIXA виступає провайдером AI-сервісу узгодженого управління мережею накопичувачів Grid Share. [10].

Згідно [3, 11-14] запропоновані подальші плани консорціуму розгорнути на базі цієї ж інфраструктури p2p-ринок для домогосподарств, мереж зарядок електромобілів, сервіси demand response, включаючи можливість участі в підтримці частоти в мережі та роботу в режимі віртуальної електростанції (VPP). Великі перспективи вбачаються у розвитку децентралізованих цифрових енергетичних технологій в пустельних державах Перської Затоки - Бахрейн, ОАЕ, Катар. В першу чергу через колосальний потенціал сонячної енергетики, на яку мало хто звертав увагу через багаті, майже невичерпні, запаси нафти та газу. У Бахрейні потужність сонячних електростанцій

становить зараз 10 МВт. Це значно менше, ніж в Україні В Об'єднаних Арабських Еміратах встановлена потужність сонячних фотоелектричних станцій становить лише 160 МВт. Десь схожі з ОАЕ показники по СЕС у Катарі. Але, вже сьогодні ці країни готуються до впровадження грандіозних планів по розгортанню сонячної енергетики та смарт-систем управління цими активами на базі цифрових технологій. І це не дивно, адже сонячна інсоляція там одна з найвищих в світі, і це їх нова нафта. Окремим цікавим аспектом розвитку децентралізованих цифрових енергетичних структур є системи життєзабезпечення відомих хмарочосів в Перській затоці.

Висновок. Таким чином, проведені дослідження дають підстави для рішення про необхідність урахування проєктів блокчейн-грід електропостачання об'єктів критичної інфраструктури та використання прикладів підсилення надійності на основі енергетичних об'єктів закордонних мереж, що мали режими роботи в форс-мажорних обставинах. Необхідно в подальшому детальніше розглянути вплив ризиків безпосередньо на самі електричні мережі, а також їх пожежну безпеку, кібербезпеку та безпеку життєдіяльності працівників критичної інфраструктури.

Подяка. Робота виконана завдяки грантової підтримки Національного Фонду Досліджень України, реєстраційний номер проєкту 0123U103529 (2022.01/0009) «Оцінювання та прогнозування загроз відбудові та сталому функціонуванню об'єктів критичної інфраструктури» за конкурсом «Наука для відбудови України у воєнний та повоєнний періоди».

1. Mylrea, M., & Gourisetti, S. N. G. (2017). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In 2017 Resilience Week (RWS) (pp. 18-23). IEEE.
2. Rudyk, Y., Bubela, T., Maciuk, K. Russia-Ukraine war: transport and logistics support for grain supply chain in regional food safety. Scientific Journal of Silesian University of Technology. Series Transport. 2023, 119, 223-233. DOI: https://doi.org/10.20858/sjsutst.2023.119.13
3. Звіт проООН. Towards a Green Transition of the Energy Sector in Ukraine JUNE 20, 2023 Update on the Energy Damage Assessment, The UNDP report https://www.undp.org/ukraine/publications/towards-green-transition-energy-sector-ukraine
4. Тріщ Р., Горбенко Є., Доценко Н., Кім Н., Кіпоренко А. Розробка кваліметричних підходів до процесів системи управління якістю підприємств згідно з міжнародними стандартами ISO серії 9000. Східно-Європейський журнал передових технологій, 4(3), 2016, 18-24.
5. Білик С.І., Петровськитй В.Л., Рудик Ю. І. Адаптація систем оцінювання за показниками безпеки в умовах особливого періоду. Охорона праці: освіта і практика. Зб. наук. праць III Всеукраїнської науково–практичної конференції викладачів та фахівців–практиків, Львів, 2023. С.50-54.
6. Білик С., Бубела Т., Рудик Ю. Оцінювання ризиків об'єктів критичної інфраструктури. Міжнародна науково-практична конференція «Інформаційно-вимірювальні технології ІВТ-2022»: тези доповідей, Львів, 2022. С.32-35 Режим доступу: https://science.lpnu.ua/ivt-2022/proceedings-2022.

7. Smart Grid та організація інформаційного обміну в електроенергетичних системах / О.В. Кириленко, І.В. Блінов, С.Є. Танкевич // Технічна електродинаміка. 2012. № 3. С. 47-48.
8. Svitlana Bondarenko. Smart Grid in ensuring the intellectualization of the energy system of Ukraine. URL: https://paperssds.eu/index.php/JSPSDS/article/view/85
9. Олійник Д.І. Міжнародний досвід високотехнологічного економічного розвитку на основі побудови smart grid. URL: http://surl.li/mlynr
10. Josue Campos do Prado, Wei Qiao, Liyang Qu, Julio Aguero The Next-Generation Retail Electricity Market in the Context of Distributed Energy Resources Vision and Integrating Framework. URL: http://surl.li/mlyom
11. Шість інновацій розподільчої мережі майбутнього. URL: https://vsenergy.com.ua/categories-page/shistinnovacij-rozpodilchoi-merezhi-majbutnogo/
12. Розподілена генерація. URL: https://zakon.rada.gov.ua/laws/term/38583
13. Розподілене виробництво енергії. Переваги та можливості для кожного українця. URL: https://ecoaction.org.ua/rozpodilene-vyrobnyctvo-energii.html
14. Енергетична безпека України: методологія системного аналізу та стратегічного планування. Аналітична доповідь. Київ 2020.

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2023»

Збірник матеріалів конференції

28-29 листопада 2023 р.

Usage of blockchain technologies in energetics – 2023 : collection of materials of the scientific and practical conference, Kyiv, November 28-29, 2023, PIMEE of NAS of Ukraine. - 2023. - 72 p.

Використання блокчейн технологій в енергетиці – 2023» 2023 : збірник матеріалів науково-практичної конференції, м. Київ, 28-29 листопада 2023 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2023. – 72 с.