ІННОВАЦІЙНІ ПІДХОДИ ДО ПРОФЕСІЙНОЇ ОСВІТИ НА ЗАСАДАХ СТАЛОГО РОЗВИТКУ

УДК 37.012:519
DOI 10.33251/2522-1477-2021-9-134-139

БОНДАР Ольга Петрівна,
кандидат фізико-математичних наук, доцент, доцент кафедри фізико-математичних дисциплін, Льотна академія Національного авіаційного університету
ORCID 0000-0001-5877-5667

СЕМЕНЮТА Марина Фролівна,
кандидат фізико-математичних наук, доцент, доцент кафедри фізико-математичних дисциплін, Льотна академія Національного авіаційного університету
ORCID 0000-0002-3567-2144

ЯКУНІНА Ірина Леонідівна,
кандидат технічних наук, доцент кафедри фізико-математичних дисциплін, Льотна академія Національного авіаційного університету
ORCID 0000-0002-0327-2349

МАТЕМАТИЧНІ АСПЕКТИ ФОРМУВАННЯ У ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ПОНЯТТЯ ПРО ДІДЖИТАЛІЗАЦІЮ

Розглянуто базові математичні параметри і операції, які утворюють сутність формування біткоіну, як одному з реалізацій діджиталізації. Наведено приклади застосування арифметики за модулем, які дають здобувачам вищої освіти, з одного боку, поняття про принципи цифрових технологій, з іншого – можливості для формування особистих умінь і навичок, необхідних у майбутній професійній діяльності.

Ключові слова: *діджиталізація, цифрові технології, цифрова грамотність, криптовалюта, арифметика за модулем, біткоін.*

Постановка проблеми. В сучасному суспільстві переходу від індустріальної епохи й аналогових технологій до епохи знань і творчості поняття діджиталізації набуває все більшого поширення. Цифрові технології та цифрові інновації розповсюджуються у різних сферах людської діяльності: в освіті, медицині, економіці.

Тому сучасний фахівець повинен мати поняття про основні принципи формування цих технологій. Національна рамка кваліфікацій визначає, що здобувач вищої освіти повинен мати «уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур» [1].

Але майбутні фахівці іноді мають нечітке уявлення про принципи створення і функціонування цифрових технологій.

Внаслідок цього відбувається суттєве обмеження їх можливостей і перспектив у майбутній професійній діяльності. Відтак, проблема формування у здобувачів вищої освіти понять про основні принципи цифрових технологій є наразі нагальною.

Аналіз останніх досліджень і публікацій. Слово «digitize» означає «цифрувати (кодувати) аналогову інформацію», а «діджиталізація» – «оцифрування» [2]. В багатьох країнах світу наслідки переходу від аналогового до цифрового типу кодування інформації стали вивчатися не просто як технологічний, але й як соціальний, культурний та антропологічний процеси [3].

В Україні також відбуваються подібні процеси. Так, у 2020 році Міністерство цифрової трансформації України запустило проєкт «Цифрова освіта. Національна кампанія з цифрової грамотності».

Мета проєкту – за 3 роки навчити цифрової грамотності 6 млн українців. Для цього на онлайн-складовій проєкту розміщені безкоштовні курси з цифрової грамотності, а на офлайн-складовій – мережа партнерських центрів цифрової освіти по всій країні, де можна отримати доступ до інтернету та цифрових гаджетів [4].

Одним з важливих напрямків діджиталізації є використання цифрових технологій у фінансовій сфері. Разом з традиційними категоріями і операціями на фінансовому ринку з'явилися підходи до визначення нових категорій, таких, як криптовалюта, блокчейн, біткоін тощо.

Аналіз структури криптовалют показує, що наразі біткоіни є найпоширенішим її видом. Офіційний статус криптовалюта має в багатьох країнах [5].

В Україні регулювання криптовалюти поки не має законодавчої визначеності, хоча деякі зусилля в цьому напрямку наразі робляться. У перспективі є безсумнівним, що юридичні аспекти криптовалюти будуть регулюватися на міжнародному рівні [6]. Відтак, природнім буде зростання кількості не тільки її створювачів, а й споживачів.

Мета статті. Дати здобувачам вищої освіти, переважно, гуманітаріям, поняття про діджиталізацію, розкриваючи деякі математичні аспекти створення криптовалют на прикладі формування початкових понять про біткоін.

Виклад основного матеріалу. Фундаментальною частиною біткоіна (англ. *Bitcoin*, від *bit* – біт і *coin* – монета) є криптографичні алгоритми. Зокрема, алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) використовує еліптичні криві (elliptic curve) і скінченні поля (finite field) для формування біткоіну разом з підписом даних.

Це дає можливість третій стороні підтвердити аутентичність отриманої інформації, яка виключає, зокрема, підробку підпису.

В ECDSA для обробки інформації і перевірки її на достовірність (верифікацію) використовуються різні процедури, які включають кілька арифметичних операцій.

Протокол біткоіну містить фіксований для всіх користувачів протоколу набір параметрів:

– $y^2 = x^3 + 7$ рівняння еліптичної кривої,
– m - основний модуль поля,
– P – базову точку на кривій,
– k – порядок базової точки.

Перші три параметри задаються у протоколі і не залежать один від одного. Порядок k базової точки є функцією цих параметрів, тобто визначається ними.

Розглянемо елементарний приклад параметрів і операцій з ними у так званій модульній арифметиці, яка використовується в ECDSA.

Нехай задано рівняння еліптичної кривої:

$$y^2 = x^3 + 7$$

і дано просте число – модуль

$$m=11.$$

Тоді точками кривої за даним модулем будуть точки:

(2, 2), (2, 9), (3, 1), (3, 10), (4, 4), (4, 7),
(5, 0), (6, 5), (6, 6), (7, 3), (7, 8).

Впевнитись, що точка, наприклад, (6, 5) належить за даним модулем кривій, можна, отримавши однакову остачу від ділення на 11 значень лівої і правої частин рівняння:

$$y^2 = 5^2 = 25 \pmod{11} = 3,$$
$$x^3 + 7 = 6^3 + 7 = 223 \pmod{11} = 3.$$

Відтак, еліптичну криву за модулем m можна розуміти, як набір точок, координати яких є цілими числами від 0 до m–1.

Точки кривої можна додавати і подвоювати.

Сумою двох точок (x_1, y_1) і (x_2, y_2) є точка (x_3, y_3), для якої

$$x_3 = t^2 - x_1 - x_2 \pmod{m},$$
$$y_3 = t(x_1 - x_3) - y_1 \pmod{m},$$

де $t = (y_2 - y_1) / (x_2 - x_1) \pmod{m}$.

В результаті подвоєння точки (x_1, y_1) отримаємо точку (x_3, y_3), для якої

$$x_3 = t^2 - 2x_1 \pmod{m},$$
$$y_3 = t(x_1 - x_3) - y_1 \pmod{m},$$

де $t = 3x_1^2 / 2y_1 \pmod{m}$.

Наприклад, сума

$$(4, 4) + (2, 9) \pmod{11} = (3, 10),$$

подвоєна точка

$$2(6, 5) \pmod{11} = (2, 4).$$

Поєднання операцій знаходження суми і подвоєння називають скалярним множенням. Наприклад, точку P можна помножити на 6 додаванням її до себе 6 разів:

$$6P = P + (P + (P + (P + (P + P))))$$

або за допомогою комбінації операцій додавання точок та їх подвоєння:

$$6P = 2(P + 2P).$$

За допомогою зазначених операцій визначається порядок точки $P(x, y)$ на кривій.

Порядок точки $P(x, y)$ на кривій – це найменше ціле число k, при якому

$$kP = O(x;\infty)$$

– «точка на нескінченності».

Показником того, що в результаті скалярного множення отримано таку точку, є збіг абсцис точок P і O.

Всі програми ECDSA, пов’язані з біткоіном, використовують дуже великі числа для базової точки, простого модуля та порядку.

Їх запис у 16-ричній системі є таким:

- основний модуль m = 2256 - 232 - 29 - 28 - 27 - 26 - 24 - 1 =
  = FFFFFFFF FFFFFFFF FFFFFFFF
  FFFFFFFF FFFFFFFF FFFFFFFF
  FFFFFFFE FFFFFC2F,
- базова точка обрана таким чином, що її порядок є великим простим числом; її координати:

P = 04 79BE667E F9DCBBAC 55A06295
CE870B07 029BFCDB 2DCE28D9
59F2815B 16F81798 483ADA77
26A3C465 5DA4FBFC 0E1108A8
FD17B448 A6855419 9C47D08F
FB10D4B,

- порядок базової точки:

$$k = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141.}$$

Вважається, що ці великі значення гарантують безпеку алгоритму. Чому і ким обрано саме ці числа? Однозначної відповіді на це питання немає [7].

Наразі відомо, що вказана конкретна реалізація під назвою secp256k1 є частиною сімейства рішень еліптичної кривої над скінченними полями, запропонованих для використання в криптографії.

Зазначений процес обробки інформації використовується для так званого «підпису» даних.

ECDSA має окремі процедури підписання та перевірки. Кожна процедура – це алгоритм, що складається з арифметичних операцій.

Біткоіни існують у вигляді записів у мережі, яка називається блокчейном. Блокчейн (*block chain* – ланцюг з блоків) – побудований за певними правилами неперервний послідовний ланцюг блоків, які містять накопичену інформацію.

Копіями ланцюга блоків користується добровільна мережа підключених комп'ютерів.

«Володіти» біткоіном – означає мати можливість передати управління іншому користувачу, створивши у ланцюгу блоків запис про передачу (транзакцію) права власності.

Можливість виконувати подібні операції надається завдяки доступу до пари приватних та відкритих ключів ECDSA.

Приватний ключ – це випадкове число від 1 до порядку k. Він визначає право власності на біткоін. Відкритий ключ отримується із приватного ключа шляхом скалярного множення базової точки на значення приватного ключа. Це можна уявити у вигляді рівняння:

$$\text{відкритий ключ} = \text{приватний ключ} * \text{базова точка}.$$

Звідси випливає, що максимально можлива кількість приватних ключів (і, отже, біткоін-адрес) дорівнює порядку.

Алгоритм підписання використовує приватний ключ, а процес перевірки використовує відкритий ключ. Таким чином, треті сторони можуть перевірити справжність підпису, тоді як підписант зберігає виключну можливість створення підпису.

Операція переходу від приватного до відкритого ключа обчислювально проста. Наприклад, не вдаючись у деталі обчислень, за параметрами

$$m = 67,\ P = (2, 22),\ k = 79$$

і приватним ключем

$$d = 2$$

отримаємо відкритий ключ

$$(52, 7).$$

Дві його координати, подані у 16-ричній системі і записані у вигляді одного рядка, утворюють відкритий ключ.

Обернена операція, тобто отримання приватного ключа з відкритого, є дуже складною через великі параметри, що використовуються в еліптичній криптографії. Вважається, що для виконання такої операції сучасному комп’ютеру потрібний час, вимірний з часом існування Всесвіту.

Але з розвитком техніки і, зокрема, появою квантових комп’ютерів ситуація може змінитися.

Висновки та перспективи подальших досліджень. Розглянуті нами основи формування у майбутніх фахівців поняття про сучасні криптовалюти на прикладі створення

біткоіну показали окремі математичні взаємозв'язки, що існують між його параметрами. Це дає здобувачу вищої освіти не економічного спрямування можливість отримати початкові поняття про основи діджиталізації у фінансовій сфері, а, відтак, у інших сферах людської діяльності.

Наведені приклади застосування арифметики за модулем є простими математичними процедурами, тому їх можна вважати першим етапом засвоєння майбутніми фахівцями знань про принципи цифрових технологій.

Таким чином, розглянута послідовність викладу матеріалу визначає перспективи подальших досліджень. А саме, разом з поняттями про основи формування криптовалют здобувачу необхідно мати поняття про основи їх функціонування, про їх спільні і відмінні риси.

Це, в свою чергу, має стати підґрунтям для подальшого засвоєння основ діджиталізації, надаючи здобувачам вищої освіти впевненості у можливості самостійного подальшого засвоєння цифрових технологій в інших сферах людської діяльності, і, відтак, формуючи їх особисті уміння і навички, необхідні у майбутній професійній діяльності.

Список використаних джерел

1. Постанова КМУ «Про внесення змін у додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341 «Про затвердження Національної рамки кваліфікацій»» №519 від 25.06.2020. URL: https://zakon.rada.gov.ua/laws/show/519-2020 (дата звернення: 11.01.2021).

2. Перекладаємо слово «діджиталізація» URL: https://slovotvir.org.ua/words/didzhytalizatsiia (дата звернення: 12.01.2021).

3. Тетерятник Б. С. Діджитизація та діджиталізація в контексті віртуалізації господарської діяльності. URL: https://ndipzir.org.ua/wp-content/uploads/2018/03/Teteriatnyk.pdf (дата звернення: 11.01.2021).

4. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/projects/osvita (дата звернення: 11.01.2021).

5. Как в разных странах регулируют криптовалюту: обзор законов в 2020 году. URL: https://habr.com/ru/company/moneypipe/blog/523354/ (дата звернення: 11.01.2021).

6. Модифікація конкурентних механізмів на глобальному фінансовому ринку в умовах діджиталізації. URL: https://galicianvisnyk.tntu.edu.ua/?art=743 (дата звернення: 11.01.2021).

7. An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA. URL: https://www.slideshare.net/NikeshMistry1/introduction-to-bitcoin-and-ecdsa (дата звернення: 11.01.2021).

References

1. Resolution of the Cabinet of Ministers of Ukraine "*On the introduction of changes in additions to the resolution of the Cabinet of Ministries of Ukraine from 23 leaf fall 2011 r. No. 1341 "About the consolidated national framework of qualifications*" No. 519 dated June 25, 2020. Retrieved from: https://zakon.rada.gov.ua/laws/show/519-2020 [in Ukrainian].

2. *Translated word "digitalization*" Retrieved from: https://slovotvir.org.ua/words/didzhytalizatsiia. [in Ukrainian].

3. Teteriatnik B.S. *Digitization and Digitization in the context of the virtualization of the government's activity*. Retrieved from: https: //ndipzir.org.ua/wp-content/uploads/2018/03/Teteriatnyk.pdf [in Ukrainian].

4. *Ministry of Digital Transformation of Ukraine*. Retrieved from: https://thedigital.gov.ua/projects/osvita [in Ukrainian].

5. How cryptocurrency is regulated in different countries: an overview of laws in 2020. Retrieved from: https://habr.com/ru/company/moneypipe/blog/523354/ [in Russian].

6. Modification of competitive mechanisms on the global financial market in the minds of digitalization. Retrieved from: https: //galicianvisnyk.tntu.edu.ua/? Art = 743 [in Ukrainian].

7. An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA. Retrieved from: https://www.slideshare.net/NikeshMistry1/introduction-to-bitcoin-and-ecdsa.

BONDAR Olga, The Candidate of Physics and Mathematics, Associate Professor, Associate Professor at the Department of Physical and Mathematical Disciplines, Flight Academy of National Aviation University;

SEMENYUTA Marina, The Candidate of Physics and Mathematics, Associate Professor, Head of the Department of Physical and Mathematical Disciplines, Flight Academy of National Aviation University;

YAKUNINA Irina, The Candidate of Technical Sciences, Associate Professor at the Department of Physical and Mathematical Disciplines, Flight Academy of National Aviation University.

MATHEMATICAL ASPECTS OF FORMATION IN EXTRACTORS HIGHER EDUCATION THE CONCEPT OF DIGITALIZATION

Abstract. *The basic mathematical parameters and operations that form the essence of bitcoin formation as one of the implementations of digitalization are considered. Examples of application of arithmetic by module are given, which give applicants for higher education, on the one hand, the concept of the principles of digital technology, on the other - opportunities for the formation of personal skills needed in future professional activities.*

Cryptographic algorithms are a fundamental part of bitcoin (from Bit – bit, and bit – coin). In particular, the ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm uses elliptic curves and finite fields to form bitcoin along with the signature data.

This allows a third party to confirm the authenticity of the information received, which excludes, in particular, forgery of the signature. ECDSA uses various procedures to process information and verify it (verification).

Namely, the bitcoin protocol is considered, which contains a fixed set of parameters for all users of the protocol. And also the basic operations with these parameters are considered.

We have considered the basics of the formation of the concept of modern cryptocurrencies in future experts on the example of the creation of bitcoin showed some mathematical relationships that exist between its parameters. This gives the graduate of non-economic education the opportunity to get a basic idea of the basics of digitalization in the financial sector, and, consequently, in other areas of human activity.

The given examples of application of arithmetic on the module are simple mathematical procedures therefore they can be considered as the first stage of mastering by future experts of knowledge of principles of digital technologies.

Thus, the considered sequence of presentation of the material determines the prospects for further research. Namely, together with the concepts of the basics of the formation of cryptocurrencies, the applicant must have an idea of the basics of their operation, their common and distinctive features.

This, in turn, should be the basis for further mastering the basics of digitalization, giving graduates higher confidence in the possibility of further mastering digital technologies in other areas of human activity, and thus forming their personal skills needed for future careers.

Key words: *digitalization, digital technologies, digital literacy, cryptocurrency, module arithmetic, bitcoin.*

Одержано редакцією: 12.02.2021 р.
Прийнято до публікації: 18.02.2021 р.