Lystopadova V, Khalaim D. Mathematical basis of the crypto network. *Освіта. Інноватика. Практика*, 2023. Том 11, № 3. С. 12-17. DOI: 10.31110/2616-650X-vol11i3-002

Lystopadova V, Khalaim D. Mathematical basis of the crypto network. *Osvita. Innovatyka. Praktyka – Education. Innovation. Practice,* 2023. Vol. 11, No 3. S. 12-17. DOI: 10.31110/2616-650X-vol11i3-002

УДК 339-72
DOI: 10.31110/2616-650X-vol11i3-002

Валентина ЛИСТОПАДОВА
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Україна
https://orcid.org/0000-0002-2549-8381
listopadovavv@gmail.com
Діана ХАЛАЇМ
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Україна
khalaimdiana@gmail.com

МАТЕМАТИЧНА ОСНОВА КРИПТОМЕРЕЖІ

Анотація. *Людську спільноту неможливо уявити без грошових операцій. Гроші – це специфічний термін, який є універсальним еквівалентом вартості послуг чи товарів. Історія розвитку коштів тісно пов'язана з невпинним розвитком людської цивілізації. Продукти, товари, зброя, бумажняні банкноти, акції – це всього лиш частина того, що раніше використовувалось людиною і продовжує мати попит до сьогоднішнього часу.*

Розвиток технологій не стоїть на місці. Тож нині дедалі актуальними є так звані "електронні кошти", які не випускаються національними центральними банками. Реальні гроші та монети поступово відходять на задній план. Їм на заміну стають пластикові картки та платіжні системи в мережі Інтернет.

Сьогодні спостерігається пришвидшений ріст криптовалюти. Вона є новою платіжною системою, яка має ряд переваг на відміну від інших електронних грошей. Криптовалютою користуються мільйони людей у всьому світі. Однією з причин такої популярності є сувора математична база, за допомогою якої будується біткоїн.

Математика є основою будь-якої платформи на основі блокчейну. Замість посередників, регуляторів, законів чи лідерів ці платформи покладаються на незаперечну логіку математичних моделей для створення екосистеми, яка працює для кожного користувача. Біткоїн є, мабуть, найяскравішим прикладом того, як ці моделі можуть змінити світ. Генерація монети повністю залежить від обчислювальної потужності ноутбука, що використовується для вирішення математичних задач.

У поданій статті основний акцент зроблено не лише на історії появи біткоїну, а й на математичному апараті дії криптосистеми.

Розглянуто математичні принципи роботи криптовалют на прикладі біткоїна, який сьогодні володіє найпоширенішою мережею.

Розглянуто головний інструмент криптографії, який є базовим при розробці біткоїну - еліптичні криві.

Наведено одні з основних властивостей даних кривих, а також принцип їх застосування під час створення криптовалюти.

Вказані математичні формули обчислення публічного ключа з приватного ключа.

Виділено основні причини використання еліптичних кривих, покладених в основу роботи криптосистеми.

Ключові слова: *криптовалюта; біткоїн; еліптична крива; електронні гроші; приватний та публічний ключ.*

Valentyna LYSTOPADOVA
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine
https://orcid.org/0000-0002-2549-8381
listopadovavv@gmail.com
Diana KHALAIM
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine
khalaimdiana@gmail.com

MATHEMATICAL BASIS OF THE CRYPTO NETWORK

Abstract. *Human society cannot be imagined without monetary transactions. Money is a specific term that is universally equivalent to the value of services or goods. The history of the development of funds is closely related to the continuous development of human civilization. Products, goods, weapons, paper money, shares are just a part of what was used by man and continues to be in demand to this day.*

The development of technology does not stand still. Therefore, the so-called "electronic funds", which are not issued by national central banks, are becoming increasingly relevant. Real money and coins are gradually receding into the background. They are being replaced by plastic cards and payment systems on the Internet.

Today there is an accelerated growth of cryptocurrency. It is a new payment system that has a number of advantages in contrast to other electronic money. Cryptocurrency is used by millions of people around the world. One of the reasons for this popularity is the rigorous mathematical basis on which Bitcoin is built.

Mathematics is the foundation of any blockchain-based platform. Instead of intermediaries, regulators, laws or leaders, these platforms rely on the undeniable logic of mathematical models to create an ecosystem that works for each user. Bitcoin is perhaps the clearest example of

how these models can change the world. The generation of the coin depends entirely on the computing power of the laptop, which is used to solve mathematical problems.

In the presented article, the main emphasis is placed not only on the history of the appearance of bitcoin, but also on the mathematical apparatus of the cryptosystem.

The mathematical principles of the operation of cryptocurrencies are considered using the example of bitcoin, which today has the most widespread network.

The main tool of cryptography, which is basic in the development of bitcoin, is considered - elliptic curves.

Some of the main properties of these curves are given, as well as the principle of their application during the creation of cryptocurrency.

Mathematical formulas for calculating the public key from the private key are specified.

The main reasons for the use of elliptic curves, which are the basis of the operation of the cryptosystem, are highlighted.

Key words: *cryptocurrency; bitcoin; elliptic curve; electronic money; private key; public key.*

Formulation the problem. The issue of creation and popularization of cryptocurrency from a mathematical point of view is extremely relevant. In particular, we are talking about the most famous cryptocurrency today - Bitcoin. This topic is quite important at the moment, because there is a demand in society for a decentralized alternative means of payment, which, regardless of the state and in terms of content, resembles the system of the gold standard with a limited supply of currency.

In modern conditions of digitization of all spheres of social life, virtual objects have been formed. Not everyone knows the definition of cryptocurrency, virtual wallet, bitcoin. All these things have gained considerable popularity due to the fact that without having professional knowledge and without making special efforts, you can get rich quickly.

This digital currency, which is based in turn on cryptography, is completely protected from hacking. It has no physical analogues, and its value lies in the anonymity of paying for goods and services without a commission, as well as in obtaining profit from investments.

Analysis of relevant research. The main formulations and ideas related to blockchain technologies were highlighted by such scientists as S. Nakamoto, M. Swan, D. Chiesa. The peculiarities of using a mathematical base for the formation of cryptocurrencies, the calculation of private and public keys, and the construction of elliptic curves were substantiated in his works by S. Nakamoto [4].

In 2020, Evan Malloy, in his publication Blockchain: The Mathematics of the Fundamentals, described that blockchain technology is based on more than just computer code. It is mostly closely related to mathematics [2].

In 2022, a collection entitled “Mathematics, cryptocurrencies and blockchain technology” was published, which contains a significant contribution by scientists Jose Luis Miralles-Quiros and Maria Mar Miralles-Quiros [3]. In their publication, they focused on basic mathematical and computational methods that can be useful tools for forecasting or for estimating the reasonable value of crypto-currencies.

In turn, Valtteri Niemi actively used cryptographic technologies in the blockchain theory [5]. The main goals of his work are the description of the three main features of cryptography: confidentiality, integrity and accessibility of the ecosystem in various implemented mechanisms.

When writing the article, various publications and materials on cryptography, cryptocurrencies and mathematics were analyzed. Some of my own thoughts and research are also presented.

The aim of the article. The purpose of the article is to prove about the importance of cryptocurrency in modern times and rethinking its popularity. To analyze how mathematics is used in the formation of electronic currency and wallets. Explore the basic mathematical element of cryptocurrency - elliptic curves.

Research methods. Analysis of research by scientists and methodologists, analysis of educational programs. To achieve the goal of the study, the authors analyzed scientific publications related to a) analysis of cryptocurrency systems; b) construction of elliptic curves; c) mathematical methods, tools and technologies that are the basis for cryptocurrency systems.

Presenting main material. Mathematics is a very important concept behind Bitcoin and cryptocurrency technology. Especially when it comes to protecting digital assets [1].

Bitcoin is a new decentralized payment network that started working in January 2009. This new technology was created by an author under the pseudonym or a group of authors called Satoshi Nakamoto [4]. The Bitcoin protocol is a mathematical algorithm that manages these transactions and forms a consensus among users of this system. Its main feature is decentralization, which means no organization or central structure. Network nodes are voluntary participants who enjoy equal rights and obligations. The network is open and anyone can participate. It is persistent and unstoppable.

Keeping track of cash is easy. Let us have 5 dollars. If we give 2, the result will be 3 dollars. This example shows the physical calculation of funds. But how to check whether this cash is legal, that is, whether it was minted on legal grounds? The bills would have to be physically checked to ensure their legitimacy. Counterfeiting bills is not a very difficult task, so "real money" is not a reliable thing in the twenty-first century. A cryptocurrency such as Bitcoin is significantly different from paper money. It cannot be physically counted and verified for legitimacy. So how is it even possible to keep records of cryptocurrency transactions and what ensures the security of "electronic money"? The main security components are cryptography, blockchain and mathematical principles

that track Bitcoin transactions and ensure that every Bitcoin is legitimate and no one is creating malicious transactions [6].

Bitcoin transactions are public information. Sending secret messages is a less important process than verifying information, which uses principles of cryptography and mathematics. Cryptography is the process of transmitting messages between parties, in which any outsiders do not have to understand their content [9]. This may involve the use of complex mathematics and algorithms to ensure data confidentiality, authenticity, integrity and non-repudiation.

Bitcoin is intangible and has no attachment to any currencies. Its course is extremely mobile and is determined solely by the balance of supply and demand. The circulation of this currency is not controlled by any bodies, departments or organizations and is carried out exclusively between crypto-gamers of network participants. It is not possible to cancel a coin transaction.

Bitcoins themselves are not stored centrally or locally - and therefore it is impossible to say who is responsible for their trusted storage. Bitcoins exist only as entries in a distributed ledger called a block chain, copies of which are distributed among a voluntary network of connected computers. Being the "owner" of bitcoins simply means having the ability to transfer control of these records to someone else by recording the fact of this transfer on the block chain. What gives this ability? Exclusive access to the ECDSA key pair: secret and public [10].

Blockchain is a conditionally growing ledger for recording cryptocurrency transactions. Each of its blocks consists of a hash function, which is based on the previous block, a timestamp, and the actual transaction data. The hash function acts as a digital signature that verifies that the transaction data has not been tampered with. It can be compared to a handwritten confirmation text.

A hash must meet certain requirements in order for it to be considered secure. First, it must be deterministic. That is, the same message is encoded to get the same hash:

Hello Youtube!

Hello Youtube!

79EA6E331E9F0B271400F0995EE2E0A1DB5890AEA5FA42A0275DFC6CD5BE61FA

79EA6E331E9F0B271400F0995EE2E0A1DB5890AEA5FA42A0275DFC6CD5BE61FA

Second, it must be one-sided, so it cannot be inverted or reversed. Third, it must be fast to compute. Fourth, it is not possible to find two messages with the same hash. Fifth, it must give way to an avalanche effect, that is, even with a small change in the original message, the new hash will be significantly different from the previous one:

Hello Youtube!

Hello Youtube!!

79EA6E331E9F0B271400F0995EE2E0A1DB5890AEA5FA42A0275DFC6CD5BE61FA

9774F8ECEF10CC80C45C06E7842D317E3DFFBB891D070DC8264EDCF5E5D22ED4

Not all hash functions are created equal. One of the best ways to leave digital signatures that exists at the moment is the use of cryptography, namely the elliptic curve. This allows having a 256-bit private key as secure as a 3072-bit private key using RSA protocols.

ECDSA is a certain algorithm with a public key, which is designed to create a digital signature, which is defined in a group of points of an elliptic curve [7]. It is this process that uses elliptic curves and finite fields to sign data in such a way that others can easily verify the signature. The algorithm has two procedures for signature and its verification. Arithmetic operations are the basis of every operation. The signature algorithm uses the secret key, while the verification algorithm uses only the public key.

An elliptic curve is a curve that satisfies the following equation [8]:

$$y^2 = x^3 + ax + b, \quad (1)$$

where $4a^3 + 27b^2 \neq 0$.These options prevent function complexity. They are symmetric about the x-axis and work on finite fields and cryptographic parameters, and have intuitively simple ways to add two points on a line.

In fig. 1 shows the graph of the function: $y^2 = x^3 + 7$ – the curve on which bitcoin is based (a = 0, b = 7).

In order to use this algorithm, the Bitcoin protocol must fix a set of parameters for the elliptic curve and its final field, so that these parameters are known and applied by all users of the protocol. Otherwise, everyone will solve their own equations that will not agree with each other. The parameters include the following: the equation of the curve, the value of the field modulus, and the base point that lies on this curve. An equally important parameter is the order of the base point, that is, how many times a point can be added to itself until its tangent curve becomes vertical. This parameter is selected so that it is a very simple number.

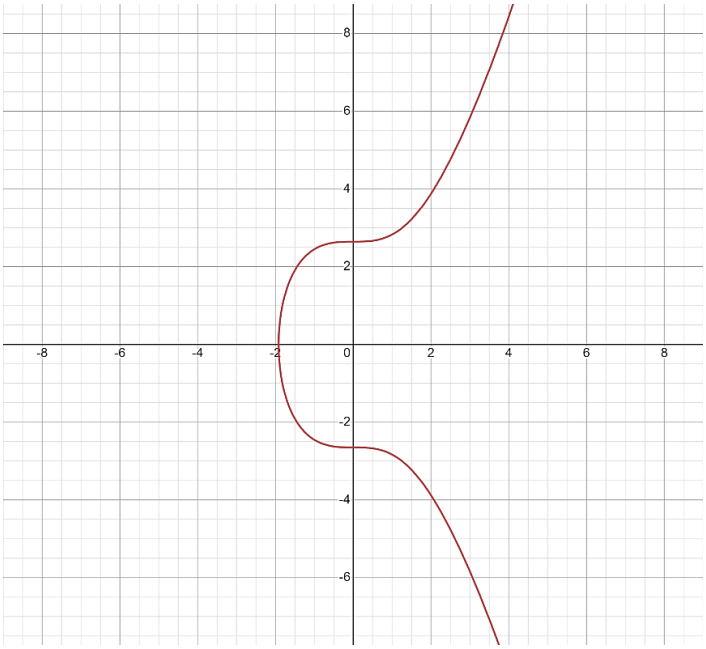

Fig. 1. Graph of the function $y^2 = x^3 + 7$

Consider the case when we need to add two units to our equation. Let's draw a straight line between them and wherever this straight line crosses the curve at the third point (Fig. 2). From this point we draw a perpendicular to the x axis.

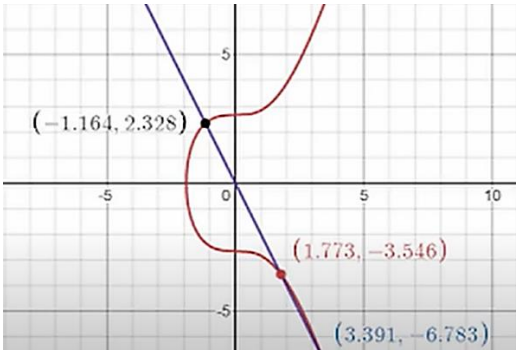

Fig. 2. The graph of the function $y^2 = x^3 + 7$, which intersects the straight line

Let point P have coordinates (-1.164; 2.328), point G has coordinates (1.773; -3.546). Then the line passing through them leads to the point (3.391; -6.783), which we will set equal to K. To get the graphical sum of these points, you need to display it through the X axis (Fig. 3):

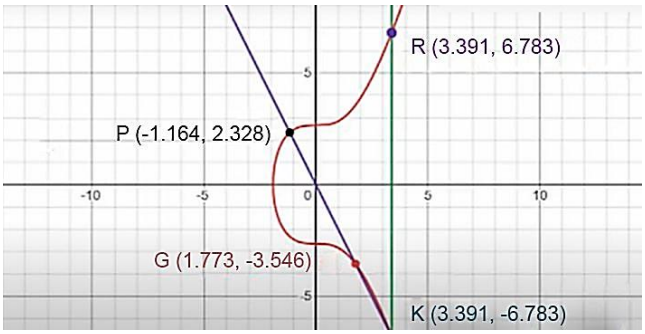

Fig. 3. Mapping point K onto the X axis

This leads to some point R with coordinates (3.391; 6.783). We see that the y-coordinate acquires a positive value. This is the sought amount. Therefore, the sum of the points is P + G = R, which we found graphically using K. However, algebraically, this is true only for elliptic curves that meet a certain condition: they act within

the finite fields on which these curves act. If we try to add P + G not graphically, we notice that the answer will not make sense (≠R) from the very beginning.

Elliptic curves work on a principle called point addition, which is significantly different from regular addition. This process involves finding the equation of the line passing through the 2 points (P, G) using the slope point form and substituting this equation for y in the original equation $y^2 = x^3 + ax + b$. The next step is to find the third root of the equation (the first root is P, the second root is G).

Let's consider another example. Let's add point P to itself twice. To do this, let's take another point and use the same curve. Let's take the coordinates of point P (-1.13; 2.357). It is chosen randomly. To add this point to itself, use a tangent line to find the coordinates of another point. This tangent is a straight line that connects the point to itself. We see that the line tangent to P crosses the curve at the point (2.92; 5.647). Displaying it through the x axis, we have the desired point with coordinates (2.92; -5.647). This reflected dot is the sought amount. Therefore, P + P = (2.92; -5.647). That is, the main principle of finding the sum is reflected by the following algorithm:

1) Finding the tangent line to the desired point;
2) Display of this point through the x-axis.

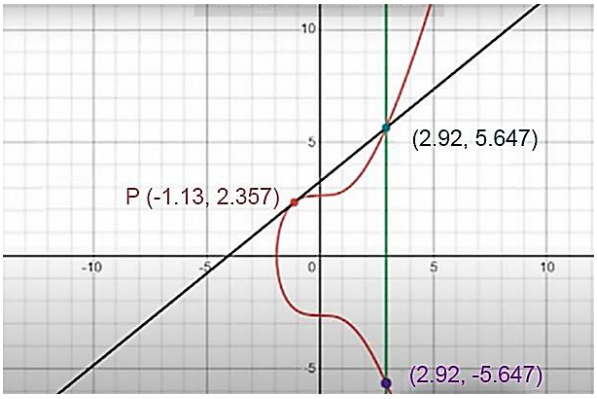

Fig. 4. Graphic representation of adding point P to itself twice

Let us have an arbitrary point on the curve P ϵ Q^2. We use this to calculate the random multiple P:

$$P + P + P + \ldots + P = nP = \left(\frac{26862913}{1493284}, \frac{139455877527}{1824793048}\right)$$

Private key Public key

This value is the private key. Since there is an infinite number of starting points and the number of times that we multiply by P, the signature is absolutely impossible to reproduce:

$$\left.\begin{array}{c} y^2 = x^3 + x + 1 \\ P = (0, 1) \\ nP = \left(\frac{26862913}{1493284}, \frac{139455877527}{1824793048}\right) \end{array}\right\} n?$$

Let's assume that the signature was solved. How to prove that he is personally ours? Everything is based on three pieces of evidence:

1) Multiplicity of the number P;
2) Calculation of obtaining a multiple number;
3) What this number was coded into.

This is called a zero-knowledge proof. Therefore, without knowing the private key, no one will be able to find out the personal data of another person. Bitcoin is a completely secure electronic currency using cryptography, blockchain technology and mathematics. It is able to keep track of all transactions that take place and guarantee that all bitcoins that are transacted will be legitimate. The math ensures that no one can go back and change the transaction. This ensures that each transaction is final, and the funds will not disappear randomly. It also guarantees that the private keys cannot be revealed by using the public key to calculate them.

Conclusions and prospects for further research. The use of mathematics in cryptocurrency fields is one of the key elements of cryptocurrency security. Mathematics helps to create unique blockchain transaction schemes, as well as to allow users to communicate with each other securely. For example, mathematical algorithms help create systems to quickly and safely transfer funds from one user to another.

Cryptocurrency continues its development these days more and more, as the number of users interested in new payment systems is constantly increasing. The demand for a currency like Bitcoin stimulates the creation

of other crypto-loots that would enjoy the same popularity. But the creation of "electronic money" would be impossible without a clear mathematical base and principles underlying its functioning. The presented article considered the main mathematical principles of cryptocurrencies and the main tool of cryptography - elliptic curves. Therefore, it would be impossible to develop a crypto network without a clear mathematical basis.

References

1. Hriunspan K. Matematyka, shcho stoit za bitkoinom. *Honka podviinykh vytrat*, 2017. S. 6-7.
2. Malloi E. *Blokchein: Matematyka za osnovamy*. 2020. URL: https://www.sdsolutionsllc.com/blockchain-the-mathematics-behind-the-basics/.
3. Miralles-Kiros Zh. Z., Miralles-Kiros M. M. *Matematyka, kryptovaliuty ta tekhnolohiia blokchein*. Bazel, Shveitsariia, 2022.
4. Nakamoto S. *Bitkoin: odnoranhova elektronna hotivkova systema*: monohrafiia, 2009. S. 3 – 4.
5. Niiemi V. *Matematyka ta struktury danykh u Blockchain ta Ethereum*. Turetskyi universytet, 2018. 27 s.
6. Nuhard M. Alhorytmy ta struktury danykh. *Perekhidni stany*, 2004. S. 10-12.
7. Elliptic Curve Digital Signature Algorithm. *Sait vilnoi entsyklopedii "Vikipediia"*. URL: https://uk.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm.
8. Elliptic curve. *Sait vilnoi entsyklopedii "Vikipediia"*. URL: https://uk.wikipedia.org/wiki/Еліптична_крива.
9. Filshtinskyi V.A. *Matematychni osnovy kryptohrafii*. Sumy: Sumskyi derzhavnyi universytet, 2011. 138 s.
10. Chaum D. *Slipi pidpysy dlia nevidstezhuvanykh platezhiv*, 1983. 199-203.