CRYPTOCURRENCIES AS THE FUTURE OF MONEY:
THEORETICAL ASPECTS, BLOCKCHAIN TECHNOLOGY AND ORIGINS OF CRYPTOCURRENCIES

Marta Ciarko, Greta Poszwa, Agnieszka Paluch-Dybek, and Mustafa Caner Timur

Abstract. During times of technological development, many aspects of everyday activities have been digitalized while traditional forms of payments have stepped back in the name of more innovative methods such as cryptocurrencies. This article focuses on analysing the emergence, functionality, and future role of cryptocurrencies, particularly Bitcoin. By interpreting the theoretical aspects of money, the emergence of cryptocurrencies, and blockchain technology, the authors tried to determine whether cryptocurrencies have the potential to become the money of the future. In the article, the analysis of cryptocurrencies’ functioning in the modern world focuses on the role of technological development and innovations in their use and popularity. SWOT and speculative analyses of cryptocurrencies, which have been touted as the money of the future, were also carried out. The results obtained from the research show that cryptocurrencies have many advantages over traditional payment methods. Elimination of intermediaries, low transaction costs, safe storage of data, limited increase in monetary supply, globalization, and privacy are stated as the most important of these opportunities. In addition, energy use, inaccessibility without the internet, high volatility, and cyber-attacks were seen as the most important threats and weaknesses. When developments in the world follow, it can be seen that there are many blockchain-based opportunities or threats. Despite this, blockchain technology offers great opportunities. As a result, countries and individuals should turn to this technology now to benefit more in the future. At this point, it is very important for all other educational institutions, especially universities, to implement educational programs that will meet the needs of the age.

Keywords: blockchain; digitalization; economy; cryptocurrency; bitcoin; exchange tools.
Authors:

Marta Ciarko
Stanislaw Staszic State University of Applied Sciences in Pila, Pila, Poland
E-mail: mciarko@ans.pila.pl
https://orcid.org/0000-0001-6690-3833

Greta Poszwa
Stanislaw Staszic State University of Applied Sciences in Pila, Pila, Poland
E-mail: gposzwa@gmail.com
https://orcid.org/0000-0003-2508-2199

Agnieszka Paluch - Dybek
The Jacob of Paradise University, Gorzow Wielkopolski Poland
E-mail: apaluch-dybek@ajp.edu.pl
https://orcid.org/0000-0001-5719-1133

Mustafa Caner Timur
Ardahan University, Ardahan Turkey
E-mail: mustafacanertimur@ardahan.edu.tr
https://orcid.org/0000-0002-3259-8495

Corresponding author: mustafacanertimur@ardahan.edu.tr, mciarko@ans.pila.pl

1. Introduction

In a fast-paced world full of innovation and new technologies, more and more classic aspects of everyday life are being transferred to the virtual realm through Internet access. The digitization of daily habits and behaviour has become an everyday occurrence [1]. As a result, such basic things as money are also undergoing a digital revolution. Traditional forms of payment are giving way to innovative solutions that are revolutionizing the way transactions are made and value is stored [2]. One of the most rapidly growing areas in this field is cryptocurrencies. Their creation and development over the years is a fascinating subject that deserves in-depth study. Their future, however, like any revolution, is in question. Thus, the purpose of this study is to answer the question of whether cryptocurrencies are the money of the future or just speculation.

A complementary analysis of cryptocurrencies was made, with emphasis on their origins, functioning, and prospects. In particular, the work will focus on studying the flagship cryptocurrency Bitcoin, which has become a symbol of a revolution in finance and technology. It is assumed that blockchain technologies, which are considered a fairly new field, will become more important in the digitalised world. Although blockchain technology is mostly heard of with cryptocurrencies today, it is expected to be used in many areas in the future. These areas can be summarized as health, insurance agreements, notary services, supply chain management, finance, voting, media, real estate, art collecting, and many public services. Although blockchain technology is not sufficiently perceived in our lives right now, some countries such as Estonia, Malta, the United Arab Emirates, Singapore, and Georgia have already accelerated their work on the mentioned issues.

The authors of this paper assume that the emergence of cryptocurrencies, especially Bitcoin, is just the beginning of blockchain technologies. The possibility of seeing digital currencies of blockchain-enabled central banks in the future makes this field even more valuable. However, while there are relatively few academic articles on cryptocurrencies and blockchain technologies, there are many speculative texts. Therefore, the studies carried out in this field today will enlighten the way for those who will research the subject in the future.

Also, it is very crucial to examine the cryptocurrency market, which had a market volume of 3 trillion dollars at its peak, from an academic perspective and to make some inferences. Properly analysing cryptocurrencies as an innovative form of money and understanding their impact on society and the economy requires an in-depth study of various aspects, from theoretical basics to practical implications. The authors of this publication intend to provide information following their analysis of cryptocurrencies, particularly Bitcoin, in the context of their origins, functioning, and prospects. In addition, this study, which evaluates the development of monetary systems, aims to satisfy the practical interest of enthusiasts. From an academic perspective, The paper aims to contribute to the field by analysing cryptocurrencies using the SWOT analysis.

2. Literature review

Marta Ciarko, Greta Poszwa, Agnieszka Paluch-Dybek, and Mustafa Caner Timur
Virtual Economics, Vol. 6, No. 3, 2023
2.1. History and Evolution of Means of Payment: Selected Aspects.

The literature on the subject indicates that both the origins and evolution of money are complex and varied, not only because of the multiple definitions of it, cultural differences, and geographical location but also the period in human history. The history of means of payment is as extended as the history of commerce itself, and it is essentially impossible to specify the exact date of its beginning, but thanks to historical sources, it is estimated that as early as several thousand years B.C., transactions were based on exchange trade, and later also with the help of various types of means of payment, which eventually, over the following centuries, evolved into the money known today.

When looking for the origins of money, it is necessary to go back to the beginning of the Neolithic Revolution. For centuries, primitive peoples provided themselves with the goods necessary for their existence by hunting animals or gathering what the land and the sea brought out. At times, when a specific area was exhausted, they moved to another location in search of new resources. However, over time they were able to domesticate animals and discover the basics of plant cultivation. People learned to produce food themselves, and this enabled them to abandon their nomadic lifestyle. Initially, primitive methods of cultivation and farming only allowed them to fulfil their own needs. This was the so-called natural agriculture. Thanks to the development of agriculture, harvests became more and more abundant, and producers were unable to use them for their consumption. The resulting surpluses became one of the first elements of the emerging trade. The surplus stock of one party was exchanged for the stock of the other, and in this way, both parties of the transaction benefited from it. The system of trade thus described is referred to as barter. Popli and Jain (2016) define it as the direct exchange of goods and services, or more precisely, the exchange of one commodity for a certain amount of another. It is pointed out, however, that making a barter requires the parties to meet certain conditions. First, there is highlighted the need for a double alignment of needs [3] also referred to in the literature as a double alignment of interests [4].

As early as 9000 B.C., the first form of money was animals such as cattle, sheep, and camels. The sedentary lifestyle of early nomadic peoples aroused the desire to own, so people began to grow their own grain, and vegetables and produce the first products, which over time became valuable commodities for barter. In some parts of the world, beads, skins, bones, or teeth of wild animals were valuable items [3].

In ancient Egypt, barter was prevalent; larger transactions were settled with precious metals such as silver or gold "by weight." The basic unit was the debenture weighing about 90 g and divided into 10 parts of lesser value. The price difference between the two metal types was not significant. The estimated ratio of the value of silver to gold was about 1:1.56. In small transactions, copper bars called oaten were also used. Ceramic assigns were also known, confirming an obligation, on which its value was inscribed [3].

Barter, despite its usefulness, was not the only form of payment in the emerging and evolving trade. Due to its numerous disadvantages, it became necessary to use universal means of payment. Thus, the so-called commodity money was created. The objects that performed their function varied depending on the community in which they were used and their availability in a particular region of the world. As an example of commodity money, S. Kubiczek mentions...
wampum. These were strings of beads with piled-coloured shells, used as means of payment by North American Indians in the 17th and 18th centuries [4].

Around 2,000 B.C. in China, small, light-coloured shells called *kauri* [77] began to be used as a means of payment. Other examples of commodity money include whale teeth, used by Fijian islanders, tobacco used as a form of payment in North America during colonial times [78], and stone circles from Yap Island in the Pacific [4]. The invention of coinage is attributed to the Phoenicians, but the subject's sources indicate, that the first pre-minted coins appeared almost simultaneously in Lydia (Asia Minor, today's area of Turkey) and Argolid in the Peloponnese [5]. However, it should be noted that the contribution of the Phoenicians to the development of international trade, as well as to the means of payment itself, was considerable, since they are responsible for the first system of transactions, with features of cashless settlement. In order to make them, the Phoenicians used authenticating plates, which were a tool for conducting financial operations.

The spread of coins as the default means of payment was quite rapid. The invention from Lydia made its way to Greece, where coins began to be minted on a wider scale. From there they made their way to Sicily and more Mediterranean countries. However, as the use of coins became more widespread, the problem of determining their value arose, as coins made of different precious metals began to exist on the market. Then it became necessary to determine the ratio of the value of silver coins, used for everyday transactions, and gold coins, generally used on special occasions. Such a proportion is called parity today, and it was first used by the Greeks and Romans back in ancient times.

Another turning point in the history of forming means of payment, used until modern times, was the emergence of the idea of token money. This money is also referred to as fiduciary and fictitious money. In the literature, it can also be found under the term *fiat money* [6]. This is money, appearing in the form of coins and bills, the purchasing power of which does not depend on the value of the material from which they are made. "The purchasing power of token money is due to the fact that it is declared by the state authorities in a given country as the valid means of payment" [7]. Early forms of paper money also functioned in the Middle Ages. They appeared in the form of merchant's letters or bills of exchange, which could be exchanged for a corresponding amount of precious metal. The Swedes are considered to be the precursors of the use of paper money in Europe.

Paper money is directly related to token money. Paper money, which does not have a direct reflection on precious metals, is still in effect today. However, this fact does not prove the absence of disadvantages of such an arrangement. After all, the introduction of paper money had some shortcomings, which are described by S. Kubiczek. The author indicates that the said type of money created the necessity of issuing it by just one superior entity - the state, having monopolistic or oligopolistic privileges in this regard. Such an arrangement was supposed to ensure the stability of the financial system. However, in such an arrangement, the state's exclusive possession of the right to create money could have created a temptation to abuse the powers it received and use them to generate its profits [4]. The first paper money in Europe was created in the 17th century. Specifically, the first known example of paper money came from Sweden and was issued in 1661. It was a bank bill worth one bank ducat, which was introduced by the Swedish Riksbank [8].
The turn of the 20th and 21st centuries was a time of rapid growth in the number of different means of payment operating on the market. The rapid development of technology resulted in the emergence of completely new solutions in the sphere of finance and payments. A turning point in the modern history of means of payment was the introduction of electronic money. It made it possible to store value "in the form of a record on a computer disk" [4], which is a more convenient alternative to cash. Since the advent of scriptural money, existing as an electronic record on an account, people have begun to invent ways to transfer value that do not require the involvement of physical money. It should be mentioned that the multiplicity of new technologies such as wider, faster, and easier access to the Internet, the development of telecommunications technologies, and new innovative payment methods such as BLIK are encouraging the emergence of new cashless payment solutions.

In conclusion, the authors of this study agree with the approach that the most general and neutral definition of money seems to be the view that it is simply anything that has been recognized as a medium of exchange and this can be classified as one of the following forms, such as commodity money, depository receipts, fiat money, fractional money [9]. It is worth presenting, in the opinion of the authors of this document, a panel study conducted in 2018 on behalf of the Cashless Poland Foundation, which shows the change in consumer payment behaviour in 2020 and the following year, 2021. The results of the study are shown in Figure 1. In the first surveyed year of 2018, most retail transactions performed at stationary retail and service outlets were carried out with cash (57%). Competing with cash in the survey presented were non-cash forms of payment. In subsequent surveys, the share of cash in the total number of transactions declined until 2021 when a larger share of transactions at retail points was in favour of the cashless form of payment. This rate of change in payment habits is seen by the Cashless Poland Foundation as evolutionary. The reasons are pointed out, among others, because of the generational change and the general popularization of digital technologies [10].

The number of transactions without the use of physical money, which is steadily increasing, building the ground for the development of new forms of payment, is presented below for better illustration. One of them is the emergence and development of cryptocurrencies.

![Figure 1. A share of payment types in the number of point-of-sale transactions in Poland 2018–2021. Source: developed by the authors based on [92]](image-url)
improve existing payment systems, as well as those that introduce completely new products directly related to finance. One of these payments is electronic payment methods, which have various types today, such as cryptocurrency.

2.2. The emergence and specification of Bitcoin's flagship cryptocurrency.

Reflections on cryptocurrencies should begin with their definition, which, however, poses numerous problems. The literature on the subject shows several different explanations of it, which indicates the unclarity of this concept. This feature is particularly highlighted by the fact that cryptocurrencies, as well as the technology associated with them, are the subject of consideration in many radically different scientific fields, ranging from finance and accounting to computer science and law. Moreover, the name of cryptocurrency itself is not the only term to describe the phenomenon. S. Peng used the term digital currencies [11], in turn, in the deliberations by E. Wiszniowski there appeared virtual currencies [12], and the phrase cryptocurrencies mentioned at the beginning is used in the text by G. Sobiecki [13], as well as the book by A.I. Piotrowska entitled "Bitcoin. "Bitcoin Payment and investment applications of cryptocurrency" [14]. The quoted terms were cited in the work by P. Druszcz, suggesting that despite their common use as synonyms, the literature on the subject shows some differences between their definitions [15].

The first type, the most basic, is cryptocurrencies used for payments. Their use is limited to a means of exchange or storage of value. An example of such a cryptocurrency is Bitcoin (BTC). However, it should be noted that since its value has risen sharply, micropayments made with it have begun to be unprofitable, due to the high cost of transaction fees. However, it has remained an investment instrument and a form of capital storage. Other examples of digital currencies typically used for payments are Ripple (XRP), Tether (USDT), Waves, Algorand (ALGO) and Avalanche (AVAX), Ethereum (ETH). The situation with the rise and popularization of cryptocurrencies can be safely compared to the medieval period, when the wealthy were able to mint new coins, thus generating inflation. At the time, such activities left their mark mainly on merchants, who, in order to normalize the situation, established their organizations called guilds. Which eventually resulted in the creation of their own currency used throughout Europe. This currency was created for their needs and was neither issued nor controlled by the authorities [16].

Bitcoin is often considered the first cryptocurrency, but similar ideas have appeared earlier [17]. D. Chaum, an American mathematician and computer scientist, is considered one of the pioneers in the field of cryptography and computer security [18]. In the 1980s and 1990s, he was involved in developing the concept of anonymous digital transactions and devised several key algorithms, such as floating-point encryption and digital signatures. In 1982, D. Chaum had an idea for his version of a cryptocurrency that is a form of anonymous transfer. In addition, he created his concept of Blind signatures for untraceable payments, which he made public at the University of California's computer science department. In 1983, D. Chaum founded DigiCash, which was one of the first companies in the world specializing in electronic money transfer. Today, D. Chaum is considered one of the most influential pioneers in the field of digital currency and is referred to as the "father of digital currency." The online platform of the same name created by him gave the possibility to make transfers between users. All you had to do was launch the program and charge your account with a transfer from your bank. The system
converted the sent real currency into "cyber dollars." The premise was the anonymity of the transactions. The company was to generate profits from licensing this technology, however, the system by its centralization was very vulnerable to hacking attacks thus losing trust in the eyes of customers, and in 1998 the company went bankrupt [79].

Sources indicate that on January 8, 2009. S. Nakamoto (a pseudonym used by the person who created the Bitcoin cryptocurrency published the Bitcoin software) published the Bitcoin software, but the cryptocurrency's blockchain came into existence on January 3, 2009, and that is why this date is considered the birth of Bitcoin because that is when the first block in the blockchain was approved at that time. Fundamental is the fact that Bitcoin is not only a blockchain, but it is also a set of concepts, technologies, the corresponding protocol, algorithms, and network [19] (Figure 2).

Figure 2. A Brief Chronology of Cryptocurrency and Bitcoin
Source: developed by the authors based on [25;86;87;93].

The whole thing is deceptively similar to the original version of the Internet, and yet the other is not the Internet. To enjoy the benefits of the Web, all you need to do is to install a browser, the choice of which is now very large. If someone knows how to program, he can create his own. The same is true with the software for Bitcoin cryptocurrency - everything will work if it follows the protocol, which is public. The literature states that one of the main advantages of Bitcoin is open source, which means that anyone can learn the principles of its operation down
to the smallest detail. This makes it possible to create communities and attract new "miners" [20].

Authors V. Dhillon, D. Metcalf, and M. Hooper [21], describe Bitcoin as a breakthrough because it features an innovative double-spending security feature that has worked for more than a dozen years. An important feature is that its creator is the same user of the network and, like the rest of the users, does not have, any additional perks. This aspect distinguishes this cryptocurrency from previous similar projects, whose creators cared about having an income if only for being their creators. This solved the problem of "Byzantine generals," i.e., detecting an element, in this case, a node of the network, i.e., a single user who is intentionally acting incorrectly. This could have turned out to be difficult since network users are all equal. Although most holders of cryptocurrencies have not heard of this problem, it is important to know that its solution has proved to be a breakthrough in their development [21].

Cryptocurrencies, including Bitcoin, are decentralized, which means that there is no single entity or institution that will exercise control over the transactions performed [22]. Also key to the concept of cryptocurrencies is the fact that access is not geographically restricted, and no supervisor is indicated in their trading by which there is no possibility of third-party interference cancelling a transaction or taking over another account by the power of its law [23]. Users connect to the network without middlemen. Each of them has equal rights, and the blockchain exists in tens of thousands of copies. Even the failure of thousands of computers responsible for approving transactions will not cause problems, unlike in a traditional bank where the failure of one device can cause problems for all its customers [24].

The authors of the literature claim that Bitcoins, like most of the resources available on Earth despite their virtual form will run out in the future [25]. The maximum amount of BTC that "miners" can "dig up" is 21 million. Such a limitation is placed in the network's protocol and has been present since its emergence. Since the creation of BTC with each block created was 50 BTC going to the address of the miner, in 2012 after the reward decreased by half, such an event is called "halving" from the English word – half [26]. At the time, one Bitcoin was valued at $12.5. Another halving of the reward from 25 to 12.5 BTC took place in 2016, and at that time the said cryptocurrency was valued at $650 per unit. The following year it soared to an astronomical level of more than $19,000 [27].

Creators and investors predict, the next halving of the reward will occur in 2024 and will drop to the level of 3.125 Bitcoin. According to the protocol for the operation of the BTC network, halving follows the mining of another 210,000 blocks. The last halving is not expected until after 2100 - this has to do with the increasing difficulty of digging up more Bitcoins while reducing the total supply of the virtual currency (21 million). In the 11-year history to date, more than 18 million Bitcoins have already been mined [28].

3. Methods

The selection of the right research method was considered based on several criteria. The problem with choosing the right research method for cryptocurrency analysis is mainly due to the multi-criteria nature of choosing the right method. At each stage of the decision-making process, the authors of this study undertook a discussion of the choice of one of many options,
each of which was considered from the point of view of multiple criteria, and these represent different values for those involved, which is undoubtedly related to the varying nature of the various elements. They should undoubtedly be taken into account in evaluating the selection of the optimal and appropriate, from the point of view of each criterion, solution.

By analysing the theoretical aspects of money, the origins of cryptocurrencies, and blockchain technology, the authors identify the future potential of cryptocurrencies. Thus, the research problem addressed in the article was considered based on the theoretical context aimed at indicating the theoretical framing of the issues taken up in the article and their interpretation and indication of their relevance, as well as an attempt to establish a theoretical and methodological pattern of conduct as a starting point for implementing a research project aimed at enriching the existing discussions in this area.

4. Result

4.1. Cryptocurrencies as money of the future

The progress observed in recent years in the computerization of societies has led to the transfer of more and more aspects of everyday life into the realm of virtual reality [29]. This process has led to the emergence of many previously unknown phenomena, including those related to the economy. One of the innovative products of human thought, existing only in virtual reality, is cryptocurrency which Bitcoin and Ethereum represent. They are among the first and the most widely used e-currency. Bitcoin is intended to be an entity distinguished by its independence from central banks, and its value is to be formed solely based on market mechanisms [30].

The rudimental theoretical justification for creating a virtual currency is based on the economic doctrine of the Austrian school, which concentrates on the analysis of business cycles and monetary theory. Proponents of this school maintain that interventions in currencies are the cause of business cycles and that excessive credit expansion caused by the fractional reserve system leads to a surge in the money supply and artificially low interest rates [31]. A paramount source of information on the future of money is Friedrich Hayek's book, in which the author argues for the abolition of the state's monopoly in issuing money. He implies that commercial banks should have the right to issue interest-free certificates that would be tied to their commercial brands [32].

Another work relevant to the topic is the work by Jesús de Soto, which proposes to introduce the concept of free banking, which promotes free trade and freedom of financial services. This concept aims to constrain state and central bank interference in the issuance and control of the value of money. The idea includes replacing paper money with gold, introducing a free banking system, and abolishing the central bank [33]. These urges have been reflected in the cryptocurrency system, which operates exclusively in cashless circulation. The situation in Japan, where there was a shortage of 10,000-yen bills, prompting the Japanese central bank to introduce more than a billion new bills a year, can be taken as the source. In this context, Bitcoin is seen as a suitable starting point for dismantling the monopoly of money issuance by central banks. At the same time, it is intended to be the opposite of the current partial reserve-based system and to refer to the earlier gold standard [34].
Many researchers are looking for the answer to the question of what the monetary ideology in the Bitcoin system is. It is possible to find the answer to this question in Bitcoin’s whitepaper and its first block called Genesis. Nakamoto stated in his whitepaper that third parties needed to establish trust to increase costs. In addition, he gave messages that sometimes he could not establish trust in existing people or institutions to ensure trust. One of these messages is "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." is the message [81]. Due to this and the messages published later, different meanings have been attributed to Bitcoin as a rebellion against the existing system. One of these meanings is the suggestion that the rescue of the banks following the 2008 financial crisis—a socialist solution to a capitalist problem—was essential in the development of Bitcoin [83]. After the 2008 crisis, the bailout packages were prepared with the taxes of the people and because of the decreasing trust, Nakamoto (2009) made the following evaluation of the currencies under the control of the Central Banks: “The root problem with conventional currency is all the trust that is required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy and trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.”

As Nakamoto stated, especially because of the decisions taken by US President Richard Nixon in 1971, because of the detachment of the dollar from the gold standard and the steps taken in the following processes, the markets became more dependent on liquidity credit. In a world with limited resources, this situation has given financial markets unlimited growth opportunities with derivative instruments that have increased over time [85]. Due to the unchecked use of these opportunities, the actual economy became separated from the paper economy, which led to enormous debts from businesses and households that could not be expected to be repaid, which in turn caused the 2007–2008 financial crisis and the governments [82].

Bitcoin is a flexible medium of exchange that can now be used to make payments for a growing variety of goods and services. It is straightforwardly accessible from anywhere in the world [35]. All that is needed is an Internet connection, skipping the need for banks and intermediaries, and avoiding costly commissions, limits, and restrictions. Another advantage of this digital currency is the lack of the need to fill out forms at the bank or post office, the critical is the bitcoin address that will enable the transaction. There is a fierce debate in the public space about cryptocurrencies as potential future money. They have several features that caught people's eye and sparked hopes for a revolution in financial systems. Here are some arguments about cryptocurrencies as the money of the future [36]:

- Decentralization and independence from financial institutions: Cryptocurrencies are based on blockchain technology, which allows them to operate without a central controlling authority. As a result, they are features with a high degree of independence. They do not indicate any dependence on traditional financial systems and institutions, such as banks or governments.
- Swiftness: Payments in Bitcoin are made online. In the process of transferring funds, the distance of the place where the money is sent is irrelevant, and the transaction takes place without intermediaries. Bitcoin transfers have no restrictions in terms of days of the week or holidays, funds can be sent 24 hours a day, seven days a week. Transactions are approved virtually every 10 minutes.
• Global reach: The availability of cryptocurrencies is unlimited in time and geography. They remain available to users worldwide and have no territorial restrictions [37]. This makes them a versatile payment tool, easily used to transfer money to and from anywhere in the world. To open an account and acquire cryptocurrencies, all you need to do is download the appropriate application or log in at the appropriate website assign a password, and login. Users of the system remain anonymous.

• Transaction security: The blockchain technology on which cryptocurrencies are based provides a high level of transaction security. Each transaction is recorded on a distributed network. This fact makes it difficult to manipulate and forge transactions.

• Innovation and growth potential: Cryptocurrencies continue to evolve and open the door to new opportunities in finance [38]. Along with the developing technology, more advanced cryptocurrencies are emerging that offer additional features, such as smart contracts and scalability.

Bitcoin and other cryptocurrencies are considered a revolutionary technology whose potential could swap the world of finance. According to Stephen Chapman's definition, "Bitcoin is a global decentralized virtual money" [39]. This means independence from banks, governments, and institutions, which is the foundation of security and freedom. Unlike traditional currencies (the euro, the dollar), Bitcoin is not issued through printing, thus it has no physical form. It is a system created by computer scientists around the world, using computer programs to solve complex mathematical equations [40].

The technology for creating cryptocurrencies is based on cryptography appearing as a distributed ledger system storing information about ownership in contractual units. The security against loss of ownership is a private key held by each holder preventing duplication of the unit. Holdings are linked to individual nodes in the system ("wallets"). "Wallets" are strictly protected by the private keys of anonymous users. The system of issuing and trading cryptocurrencies is based on an open network (open source) peer-to-peer. Data transfer is done through an installed application and the distribution of transfer information is the responsibility of the entire network [41].

When analysing the future of cryptocurrencies, it is worth noting both strengths and weaknesses, considering the opportunities they offer and analysing the risks associated with them. Reviewing several research tools adequate for making appropriate and accurate investment decisions, the SWOT analysis appears to be the one that will allow a thorough recognition of all conditions arising in this area. It is an effective tool used to analyse the strengths, weaknesses, opportunities, and threats of an organization, project, or product (which Bitcoin undoubtedly is), which helps address the effectiveness of product/project planning and implementation [42].

The acronym comes from an old term in the field of strategic planning, Ih refers to the content and objectives of the project and is the identification of the right things to do. SWOT analysis is a scope for a better understanding of the framework conditions (strengths and weaknesses) putting them together with the external conditions within which the project will be implemented (opportunities and threats) [43]. Due to the popularity of SWOT analysis as a tool for the accuracy and effectiveness of decisions [44], it is crucial to start the work by analysing the
critical factors in the project environment, i.e., opportunities and threats. They argue that opportunities and threats should not only be set in the present timeframe but should include a futuristic vision of the future [45]. The latter predestines SWOT analysis as an effective tool for exploring Bitcoin as the money of the future (Figure 3).

<table>
<thead>
<tr>
<th><strong>Strength</strong></th>
<th><strong>Weakness</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Lack of agents</td>
<td>1. Value based only on the trust of the system's users</td>
</tr>
<tr>
<td>2. Swift transactions</td>
<td>2. No material form</td>
</tr>
<tr>
<td>3. Low shipping costs</td>
<td>3. High volatility of the exchange rate</td>
</tr>
<tr>
<td>4. Limited maximum quantity</td>
<td>4. Vulnerable on user slips</td>
</tr>
<tr>
<td>5. 1 BTC split into 105 Satoshi</td>
<td>5. Declining reward for &quot;miners,&quot;</td>
</tr>
<tr>
<td>6. Regulation exclusively by market processes</td>
<td>6. High energy requirements</td>
</tr>
<tr>
<td>7. Protection of personal data of system users</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Opportunities</strong></th>
<th><strong>Threats</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Trade's internalization and globalization</td>
<td>1. The possibility of exploitation by the criminal world</td>
</tr>
<tr>
<td>2. E-commerce turnover boost</td>
<td>2. Hefty risk of hacking attacks</td>
</tr>
<tr>
<td>3. Mandatory (administrative) surge of USD supply and drop in confidence</td>
<td>3. Growing competition from other payment instruments</td>
</tr>
</tbody>
</table>

**Figure 3. Swot Analysis of Cryptocurrencies**
Source: developed by the authors

**Strengths**

**S.1 – No middlemen** – the elimination of middlemen in Bitcoin transactions implies speed of transactions and reduces costs. The market for cryptocurrencies is distributed which means they are available wherever the internet (and mobile telephony) is accessible. The lack of intermediaries is also associated with the decentralization of cryptocurrency issuance. The issuance mechanism is exempt from the influence of a central issuing institution and dependence on banks, governments, and institutions. In this optic, cryptocurrencies appear as supranational entities [46].

The operating model of the cryptocurrency market is essentially embedded in a P2P (peer-to-peer) network. The peer-to-peer network environment is interchangeably referred to as a peer network, and in addition, a literature search points to such terms as partner network, and collegiate network. As the name suggests, this is a network within which all computers are treated equally, without gradation. In this type of access, everyone in his "backyard" performs administrative and operational activities independently [47]. Deployment of the P2P network model in the cryptocurrency market is exposed to unattended network management solutions. Thus, no one surveys it, there is a free flow of data. The absence of a controlling entity is the absence of an entity that can derive profits in the form of a monopoly annuity [48]. A pure P2P network allows online payments to be sent directly from one party to another, without the involvement of a financial institution. Digital signatures are part of the solution, but the main benefits of cryptocurrency trading are lost if a trusted third party is still required to confirm the transaction. The need for a trusted entity to accept the transaction creates additional transaction costs. Satoshi Nakamoto has proposed a fix for the problem of double spending using a peer-to-peer network. The network timestamps transactions by hashing them in a continuous chain.
of proof-of-work, creating a record that cannot be revised without re-executing the proof-of-work. The longest string serves not only as evidence of the sequence of events but also as evidence that it comes from the largest pool of processor power [49].

S.2 – Low transaction costs – as of 09/02/2023, the fee charged for a transaction of less than 0.01 BTC is 0.000075 BTC, which is $1.6 in USD terms. Transactions for higher values are free [50].

S.3 – Speed of transactions – cryptocurrency payments are made over the Internet. It takes about 10 seconds to send a certain amount of bit money anywhere in the world, and about 10 minutes to confirm it in the system [51].

S.4 – Ultimately, the limited amount of BTC in the system – the supply of BITCOIN has been limited to 21 million units dug up. The last BTC will be "dug up" no earlier than 2140 [52].

The creator of cryptocurrencies Satoshi Nakamoto already assumed a fixed, specifically defined amount of virtual money and electronic settlements in the initial phase of creating them. He made this decision based on his analysis of current monetary systems and national monetary policies, the foundation of which is the complete freedom of central banks to print money without cover, in the amount they deem necessary. Current monetary policy models give unlimited power to a few bankers of central financial organizations and enormous influence over the fate of the rest of the Earth's inhabitants.

The principle of absolute confidence in the institutions issuing fiat currencies is a mainstay of the security and stability of the payment system of national economies [53]. History has repeatedly shown that the world's financial base relying on trust in banking systems has proved disastrous and dangerous, creating threats to national economies, shaky public finances, rising unemployment, and a decline in the quality of life of the population [54]. All these macroeconomic aspects are at play in almost every global financial crisis triggered by the protectionist policies of investment banks [55].

Lack of trust in the banking system was the reason for the creation of Bitcoin, and the idea that most likely guided its creator was to give people back their power over money. The regulated supply of cryptocurrency has very positive implications for its users [56], affects their market rate, and, unlike fiat currencies, prevents inflation [57].

S.5 – Division of BTC into smaller units – to protect the system from loss of liquidity, each BTC is divided into 100 million smaller units. Anticipating the needs of the market, the increase in the value of the currency, and the number of transactions in the created system, the introduction of smaller units was assumed [58]. A single BTC is divided into smaller units, two of which were named by using Latin prefixes [59]:

- 1 mBTC (miliBTC) = 0,001 BTC = 10−3 BTC;
- 1 μBTC (microBTC) = 0,000001 BTC = 10−6 BTC;
- 1 Satoshi = 0,00000001 BTC = 10−8 BTC.

The last smallest unit was named to honour the enigmatic creator of Bitcoin; thus, it has no Latin prefix. This is because for a unit of = 10−8 BTC such a value in Latin numerals does not
exist. The unit of 1 Satoshi filled the gap in classical nomenclature between 10^-6, or "micro," and the next-in-line unit of size = 10^-9, or "nano."

1 Satoshi = 0.00000001 BTC, or in other words 1 BTC = 100,000,000 Satoshi [60].

**S.6 – Regulation solely by market processes** – in practice, no state or organization has the authority to increase Bitcoin supply, and there are no imperatives that can trigger a devaluation of the cryptocurrency exchange rate. This is due to the lack of ties to the economy of any country.

Studies of the foreign exchange market also do not indicate that there is a correlation between the level of bitcoin quotes and the exchange rate of major world currencies and gold [61]. Inclinations to use measures describing the global economy as determinants of the value of cryptocurrencies are unreliable and unfounded. Analysis of macroeconomic indicators of national economies is not applicable here: i.e., GDP level, inflation, unemployment, public debt, and interest rates. The value of bitcoin is created by its utility function which is a bump in the possibility and degree of use in economic transactions [62].

**S.7 – Protection of personal data of the participants of the system** - the participants of the system make transactions in the form of a public key. Keys are not coherent with personal data, but the transactions carried out in the system are marked with a public accession [63].

**Weaknesses**

**W.1 – Basing the value of the instrument solely on the trust of system participants** – the value of Bitcoin depends on the demand generated by the trust of 67 system participants. It has no direct material backing, which creates a cause for criticism voiced by opponents. However, it is worth noting that the collapse of the Bretton Woods system will affect devaluations of national currencies previously backed by gold. Currently, confidence in the state is predicated on giving a currency a certain value. This allows stating the fact that the mechanisms of creating primary values (fiat currencies and cryptocurrencies) are the same in both cases. Bitcoin differs from traditional currencies mainly in that it has no centralized issuer. Its value depends largely on the trust and acceptance of the community that participates in the system [64].

**W.2 – No material form** – bitcoin currency is entirely based on electronic form. Failure of devices to access digital wallets is equivalent to blocking access. The psychological aspect of the public's lack of trust in things that have no physical counterpart appears here. The lack of a tangible form implies reduced credibility and concerns about security and stability [65].

**W.3 – High volatility of the exchange rate** – Bitcoin has a very high fluctuation against national currencies. Figure 4 shows the values of 1 BTC expressed in USD from 2019 to 2023.
Figure 4. Chart of the value of 1 BTC from 2019–2023 expressed in USD.
Source: developed by the authors based on [91]

The high volatility of the BTC exchange rate gives it a pejorative character as a medium of exchange. Entities wishing to transact in Bitcoin may opt out of this method of settlement due to the high exchange rate risk. For comparison purposes, the following is a chart of the fluctuation of the exchange rate of $1 in Euro-denominated terms over the corresponding period 2019–2023.

Figure 5. Graph of the value of US$1 from 2019–2023 expressed in EU.
Source: developed by the authors based on [90]

The value of Bitcoin fluctuates as demand increases while the amount of supply remains constant. Fluctuations in cryptocurrencies are much more capricious and drastic compared to traditional investment instruments such as gold or commodities and raw materials as expressed by the CRB index [66]. Numerous studies expose the high volatility of cryptocurrencies by relating them to the volatility and lability of the stock market [67]. Research on the correlation of bitcoin to gold and stock market prices from 2011 to 2017 [80], as well as in the period 2018 – 2022 [68], show that gold and BTC prices behave in completely different ways, especially during periods of increased market uncertainty. Gold prices are stable and show little volatility over the years analysed. They provide a foundation for hedging against risk. The volatility of cryptocurrency prices coincides with price changes in the stock markets. Due to this, the former is not recommended by many analysts as assets that can, in the wake of gold, provide a hedge (hedging) for an investment portfolio [69].
W.4 – **Vulnerability to user errors** – when transferring funds, the priority is to correctly enter the recipient's address and transaction amount. The system is simple, but it does not provide the ability to create corrections and undo an erroneous transaction. If funds are sent to the wrong address, the only possibility of recovery is the goodwill of the other party, who decides to return the received funds. Entering recipient addresses is usually done through a copy function which reduces the risk that is not eliminated by entering the recipient's address manually.

W.5 – **Declining transaction fees for those providing computing power to the system** – the fee for cryptocurrency miners, known as "miners,” is gradually declining and is projected to drop to zero in 2033 [70]. Such a scenario may lead to a decrease in interest in this activity, which will translate negatively into the efficiency of the entire system. To prevent this problem, there is a mechanism that allows voluntary payment of a transaction fee, which speeds up the confirmation of transactions and provides remuneration for "miners" [71]. This systemic protection mechanism is designed to encourage users to voluntarily pay transaction fees in exchange for faster processing of transactions by "miners." In this way, "miners" are encouraged to continue their operations despite declining fees because they are compensated by voluntary contributions from system users. This option creates smoothness and efficiency in the system, without subjecting it to disruptions and downtime in data transmission. Users have the opportunity to decide for themselves how much they want to pay according to their needs and expectations. The solution used is the simultaneous assurance of timely confirmation of transactions and receipt of rewards by "miners”.

W.6. – **High energy requirements** – cryptocurrency digging – is the acceptance of newly created blocks in the blockchain network and attaching them to a given chain of blocks in the network. The operation is based on the concept of so-called proof-of-work, which involves complex mathematical operations aimed at finding a suitable solution. Finding and adding the right solution to the chain creates an environment of competition between excavators working in the network [94]. The tool that allows you to win the race is the computing power of the device, which inevitably involves very high energy requirements. This is a factor that enters the list of weaknesses of the cryptocurrency market. Analyses conducted by De Nederlandsche Bank showed that a single Bitcoin transaction generates carbon emissions equal to those of an average family for three weeks [95].

**Possibilities**

O.1 – **Internationalization and globalization of trade** – the dynamic processes of economic and social globalization and the development of free trade zones correspond with the simplification of trade exchange processes. As a result, there is an increasing demand for a transaction system that is fast, cheap, and functional. In such a situation, the use of Bitcoin settlements can be particularly beneficial for entrepreneurs who conduct business on an international scale and make many payments to different countries. With Bitcoin, it is possible to transfer funds quickly and securely, bypassing traditional payment methods such as bank transfers, which often involve high fees and long transaction times. In addition, the use of Bitcoin makes it possible to avoid currency conversion problems, making the process of international trade payments faster and easier.
O.2 – Growth in the e-commerce segment – E-commerce is one of the fastest-growing industries. Online shopping is naturally combined with making electronic payments. Explosive interest in the e-commerce segment is in tandem with the market segment creating new, unconventional methods of electronic payments. Cryptocurrencies are unequivocally counted among these technological innovations.

![Figure 6. Share of online sales in total US sales 2010–2023](image)

Source: developed by the authors based on [89]

The large increase in the share of online sales began during the pandemic outbreak period, i.e., 2020–2021, during which the public was looking to make cashless purchases and skip personal contact [72]. As an example, Figure 6 shows the growth of the share of e-commerce expressed as a percentage in the US market from 2010 to 2023.

O.3 – Administratively increasing the supply of USD and decreasing confidence in the currency – these actions took place in 2009 during the global economic slowdown. The United States implemented a precautionary monetary policy measure known as "quantitative easing". The purpose of implementing this instrument was to stimulate the economy by increasing the money supply, resulting in a decline in confidence in the USD and a depreciation in its value on global currency markets [73]. Figure 5 shows the purchasing power of the consumer dollar in the U.S. city average from 1913 to the present. Such fluctuations in the depreciation resulting from the policy of "quantitative easing" and the associated uncertainty can change perceptions of traditional currencies and their ability to hedge against inflation. The figure below shows the described situation.

![Figure 7. Consumer Price Index for All Urban Consumers: Purchasing Power of the Consumer Dollar in U.S. City Average, Index 1982-1984=100, Monthly, Not Seasonally Adjusted](image)

Source: developed by the authors based on [88]
The described model of how the market reacts to changes triggered by the imperative of monetary policy appears as an opportunity for alternative instruments, such as cryptocurrencies, which in their original conception, are intended to protect their holders from inflation. They are independent of traditional monetary systems and not subject to direct administrative manipulation of supply. Thus, holders of cryptocurrencies have the opportunity to protect their assets from the negative effects of inflation, which can result from government actions or other external factors.

**Threats**

**T.1 – Potential for widespread use by the criminal world** – The high level of anonymity especially for users who do not exchange Bitcoin for traditional national currencies may pose a risk that the system could be used for illegal purposes, such as trading in prohibited goods or financing terrorism. Since Bitcoin transactions are not subject to administrative control, there is also a high probability that cryptocurrencies can be used for "money laundering." Due to these negative aspects, there is a risk of authorities acting to outlaw Bitcoins to prevent such irregularities. It is worth noting, however, that an increasing number of online currency exchange offices and exchanges that have a service for exchanging Bitcoins for traditional national currencies require their customers to provide personal data. This allows users to be identified and can reduce the risk of illegal use. The introduction of identification procedures is an attempt to regulate the cryptocurrency market and make transactions more secure. However, it should not be forgotten that many other channels allow anonymous transactions to continue. For this reason, further efforts are needed to monitor and regulate the cryptocurrency market to ensure security and eliminate illegal practices [74].

**T.2 – High probability of hacking attacks on vital nodes of the system** – There is a high probability of hacking attacks on some elements of the system. So far, the most spectacular one would be the June 2011 attack, it was the first digital attack on this scale, during which $8.75 million worth of Bitcoin was stolen. In 2014, $460 million was stolen similarly. Due to the design of the system, these funds cannot be recovered, and detecting and convicting the perpetrators is very complicated [75].

**T.3 – Growing competition from other electronic payment instruments** – The growth in the value of the e-commerce market is fostering the development of new facilities for the electronic trading of conventional currencies. Examples are, for example, the reduction of transaction times in ELIXIR, the PayPal payment system, SMS micropayments, or the Polish invention BLIK. They may prove more attractive to consumers because they do not require prior purchase of payment units or additional knowledge of cryptocurrencies [76].

**5. Conclusions**

As a result of the development of communication technologies and the effects of globalisation, radical changes are taking place in the economic, social, and political spheres. These changes often bring new concepts into our daily lives that we have never heard of before. One of these increasingly popular concepts is cryptocurrencies. Seen by many as a rebellion against the current monetary system, these instruments still retain their mystery and uncertainty in many ways. In addition, many investors have been victimised by the lack of regulation and legislation.

*Marta Ciarko, Greta Poszwa, Agnieszka Paluch-Dybek, and Mustafa Caner Timur*

*Virtual Economics, Vol. 6, No. 3, 2023*
Whatever the situation, this market, which became very popular and increased its economic volume, especially after the COVID-19 epidemic, has now become a sector whose importance cannot be denied. Blockchain technology, which underpins cryptocurrencies, is expected to be used in many areas in the future, from accounting to land registry transactions.

Today, many developments bring cryptocurrencies to the fore and suggest that they will reach a better position in the future. Reasons such as the US dollar, which is considered the world's reserve currency, breaking its ties with Bretton Woods, using it as a kind of weapon in the Ukraine-Russia war, and blocking SWIFT channels, bring cryptocurrencies to the fore as an alternative. In this context, the plans of the BRICS countries to create an alternative currency bring many opportunities in the coming decades. In this regard, it is very important to know the advantages, strengths, and weaknesses of the cryptocurrency market and blockchain technologies, which can be considered quite new.

Author Contributions:

Data Availability Statement: The data supporting the results of this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

Marta Ciarko, Greta Poszwa, Agnieszka Paluch-Dybek, and Mustafa Caner Timur
Virtual Economics, Vol. 6, No. 3, 2023
27. E-kursy walut, https://e-kursy-walut.pl/, dostęp na dzień 02.05.2023

Marta Ciarko, Greta Poszwa, Agnieszka Paluch-Dybek, and Mustafa Caner Timur
Virtual Economics, Vol. 6, No. 3, 2023
90. Graph of the value of US$1 from 2019 -2023 expressed in EU, Available at: https://tradingeconomics.com/ accessed 03.09.2023.