Baština Akademije nauka i umjetnosti Bosne i Hercegovine

Artificial Intelligence in Industry 4.0: The future that comes true: AI

Karabegović, Isak; editor

2024-09-17

https://bastina.anubih.ba/handle/123456789/791

Preuzeto s Baštine Akademije nauka i umjetnosti Bosne i Hercegovine

https://bastina.anubih.ba/

DOI: 10.5644/PI2024.215.11

The Role of Blockchain Technology in the Transformation of Digital Marketing

Savo Stupar[*1], Elvir Šahić[1], Maida Cico[2], Mirha Bičo Ćar[1]

Abstract: *With the advent of the Internet and the accelerated development of information and communication technologies (Cloud Computing, Big Data, etc.), marketing has changed forever. However, it will soon be going soon it will be going through another revolution, largely due to the potential of Blockchain technology. In order for the exchange (transaction) to be carried out to the satisfaction of both entities, there must be trust between them. Unless the entities trust each other, they usually find a solution by hiring a third entity, called an intermediary. At its core, Blockchain enables transactions between two parties without the need for third party verification. If a transaction means any business transaction of transferring ownership of goods or money (securities) from one entity to another, then Blockchain is an alternative way of exchanging and recording transactions by which it is carried out to the satisfaction of both entities, without intermediaries and without the need to trust each other. One of the more significant aspects of applying Blockchain technology is that it gives consumers back control of their personal information, eliminating the possibility for companies to take data from customers without offering them compensation. The aim of this paper is to highlight the potential of Blockchain technology, which puts customers in an even more favorable position, but also enables merchants to access non-intermediary customers such as Google, Facebook, etc. Another aspect of the application of Blockchain technology will be discussed in the paper, which concerns the possibility that customers have all relevant and true (i.e, non-changeable information due to the security provided by Blockchain technology) information about the origin of the products they purchase.*

Keywords: *Transaction, BitCoin, Blockchain Technology, Digital Marketing, Blockchain Marketing, Blockstack technlogy, Product origin*

1. Introduction

Good connoisseurs of trends in the development of new information technologies believe that the emergence of Blockchain technology represents a revolutionary technology that, due to its characteristics, contains a huge potential for changes in almost all areas of human activity, which can be manifested in improving the efficiency of performing a large number of human activities, in

[*1]University of Sarajevo, School of Economics and Business, Sarajevo
[2]International High School "Bloom"
E-mail: savo.stupar@efsa.unsa.ba, elvir.sahic@efsa.unsa.ba, maida.cico@bloom.edu.ba, mirha.car@efsa.unsa.ba

increasing or even complete transparency of these activities, eliminating the need for intermediaries (banks, state, municipality, court, prosecutor's office, lawyers, notaries, etc.) when performing a significant number of human activities, reducing the possibility of fraud and increasing the level of security in performing various types of transactions, whether they relate to the creation of cryptocurrencies and their exchange (the first application of Blockchain technology) or to the exchange of securities, documents, real estate, gems or various other goods, in trusting the accuracy and correctness of various types of records due to the impossibility of changing once stored and from a large number of equal partners, verified transactions.

Any exchange of goods (goods, services or things and money, as their measure of value) is based on transactions. Generally speaking, a transaction can be defined as the transfer of ownership of goods (things, money, real estate, jewels, securities, etc.) from one subject to another, whereby one subject (the one who initiates the transaction) loses the right of ownership of the goods, and the one who buys the goods acquires the right of ownership over them. Different names for the transaction are buying or selling, payment or spending, providing or using (services, for example), owing or claiming (on an account, for example), increasing or decreasing, receiving or giving, etc. Almost all services today are based on that concept. In order for the exchange of transactions to be carried out to the satisfaction of both entities, there must be trust between them, or if the entities do not trust each other, they usually find a solution by engaging a third entity, i.e. an intermediary, to whom, according to mutual agreement, (one or both) pay for the mediation service. Banks are the best example of this. But it is not only banks and organizations that make money from mediation services. Very often, the state, courts, lawyers, notaries, prosecutors' offices, real estate agencies, educational institutions, marketing agencies and various other institutions appear as intermediaries that manage the records of various transactions. The ultimate goal of carrying out transactions to the satisfaction of both participants in the exchange is not only the elimination of intermediaries and the avoidance of commission payments, but also the increase in security and speed of transactions, as well as the improvement and liberalization of transaction business, and the elimination of the possibility of abuse and fraud. The technology that has a huge potential to support the achievement of these goals, as well as to reduce business costs and thereby increase profits, is Blockchain technology, which is therefore considered a revolutionary technology, that is, the technology of the future.

Blockchain technology was created as an amalgam of several different, but equally revolutionary technological achievements in the field of mathematics (power of large numbers), cryptography (hash functions, which will be discussed more later), P2P computer networks (network of distributed computers or Peer to Peer network) and improvement of computer hardware characteristics, such as

processor capacity and speed, capacity and speed of access to external memory media Peer-to-Peer network (or partner network) is a distributed network made up of connected independent computers. The main characteristic of these networks is that they are constructed in a way that allows establishing a connection and realizing the exchange and joint processing of information with all other computers in the system without giving privileges to any computer in the network, that is, without a central authority. The first application of this technology refers to the support for the creation and exchange of the first cryptocurrency - Bitcoin. [1]

2. Bitcoin – First Application of Blockchain Technology

If Bitcoin did not appear, there would be no Blockchain technology. Likewise, if there was no Blockchain technology, there would be no Bitcoin. Before a brief introduction to Bitcoin, it is necessary to define some elements of the categorical (conceptual) apparatus, which are used for its explanation. Namely, the terms virtual and digital money are often used as synonyms, which is completely wrong, so it is necessary to define the essential differences between them, or more precisely the differences between virtual money and the money we use every day. Digital money is money that is transferred electronically. More precisely, it is money, the amount of which (some integer or decimal number) is stored in the computer memory in the form of a binary representation. It is the money of a user on a current account stored in the bank's computer memory, to which credit, debit cards and other cards can be attached. It is also money in the PayPal account. In this context, digital money is also virtual money, but digital money does not have to be virtual money. There are different types of digital money and different types of virtual money. Compared to traditional money, virtual money does not have all the attributes of real money. The term virtual can be defined as something that exists but is not in physical reality. Before the advent of cryptocurrencies like Bitcoin, virtual money mostly referred to money in popular MMO (Massively Multiplayer Online) games like World of Warcraft and EVE online. Bearing in mind that these computer games serve several hundreds of thousands of players who trade with each other in "raw materials and final products" in that virtual world, it very often happens that designers (game developers) ask for expert advice from economists in order to design the economic aspect of games. Virtual money in computer games is centralized, so designers (developers) of computer games can control supply and demand in the form of monetary rewards and penalties. It is important to emphasize that computer games have developed markets, which are exclusively maintained by players, and that they respond to the laws of supply and demand. The virtual markets of computer games have spawned new markets in the real world, where players can buy in-game money or goods in exchange for real money. That's

why this practice is banned in most MMO computer games, so administrators look for and punish players who engage in it by blocking their access. Virtual money suddenly gained popularity with its appearance in the form of Bitcoin in 2008, and then it was noticed by central banks in the transitional period between 2012 and 2013. The concept of virtual money is still insufficiently researched, especially from the aspect of the rapidly growing number and total value of transactions, the number of users and the extent of the confusion that cryptocurrencies caused in the regulatory systems of banks and states.

The current concept of "virtual social community" was created as a product of the rapid development of information and communication technology, globalization and the economy of virtual crypto money. Bitcoin represents the first case of the appearance of a cryptocurrency, so a more detailed look at it in the form of a "case study" from the aspect of Blockchain technology, which enabled its creation and functioning, seems necessary and useful for a better understanding of all other applications of this technology, and especially its application in the field of digital marketing.

Due to the potential of modern computers to very quickly process a huge number of transactions via a computer network, as well as due to their characteristic of possessing a "perfect and powerful memory", the idea of a decentralized currency system did not represent any novelty considering that much earlier, there were a large number of proponents of the concept of anonymous digital money.

The concept of anonymous digital money, which is considered the first wave of digital money, begins in 1981 with the work of cryptographer David Chaum on the topic: "e-mails without a trace, sender addresses and digital pseudonyms"[1]. He founded the International Association for Cryptologic Research (IACR) in 1982, and published his best-known paper entitled "Blind signatures for Untracable Payments"[2] in which he created a technical model for future digital currencies. He believed that the world needed a digital pseudo-money that would replace physical (paper) bills and metal coins (coins) and that would enable private and secure transfer of money "from hand to hand" by its design. His views on money and privacy were the inspiration for the creation of the ideology of the crypto-activist group "Cypherpunks", which was founded in 1992 and which left an indelible mark in the world of cryptography.

Back in 1991, Phil Zimmerman coined the term "Pretty Good Privacy" or abbreviated PGP, and made a free public key encryption program. For the first time, the PGP application gave every interested individual access to the enormous possibilities of cryptography, as Zimmerman printed the source code of his program in a book, which was then publicly distributed[3].

One of the main founders of the „Cypherpunks“ group, Eric Hughes, wrote the Cypherpunks Manifesto and mission statement in 1993, which read: "*Cypherpunks are dedicated to building anonymous systems...Privacy is*

essential to a free society in the modern age...We cannot expect governments, corporations and other faceless organizations to provide it to us... We must defend our privacy if we intend to have it. We defend our privacy with cryptography, with systems for forwarding anonymous emails, ***digital signatures and electronic money***."[4] The first wave of digital money in the form of an **E-cash** system as a finished product of the **DigiCash** company, was based on blind digital signatures to provide users with anonymity. Representatives of **the second wave of digital money** are **PayPal** and **E-Gold**. PayPal acts as an intermediary between the merchant and the customer, and does not reveal the customer's personal information during the transaction, because the money is actually transferred from PayPal's account. Of course, Paypal takes a fee for this mediation. E-Gold represents the first hybrid of a digital currency and a PayPal-like protocol. At the same time, E-gold is the first popular digital currency that uses gold and precious metals as collateral. Users would send money via check or card or gold or silver, and the **E-Gold** company would then allocate the currency to the user's account, as a unit of measure for the sent counter value. The **E-Gold** company would hold the physical gold, while users with e-gold currency could perform transactions worldwide.

The third wave of digital money in the form of the Bitcoin protocol is linked to Satoshi Nakamoto and the appearance of the Bitcoin cryptocurrency. When Satoshi Nakamoto, whose identity still remains a mystery, published the document "Bitcoin: A Peer to Peer Electronic Cash System“ [5] in 2008, he designed and proposed a "true version of electronic money through a Peer-to-Peer network" called Bitcoin, for the first time Blockchain technology appeared in public. In January 2009, Bitcoin is offered "open source"[2] to the public. Blockchain concept answered the question of digital trust by recording important information in the public space without allowing the information to be changed or deleted. The basic characteristics of Blockchain are: transparency, time-stamping and decentralization.

Nakamoto defined the technology that makes Bitcoin work as: "An electronic payment system that is based on cryptographic proof, instead of belief, allowing two willing parties to make direct transactions without the need for a third, independent party."[5]

To describe the meaning of the term Bitcoin, various terms are used, such as virtual and digital money, then virtual, digital, electronic, synthetic and cryptocurrency. As with most relatively recent terms, there is no single definition. The American FinCEN and the European Central Bank have designated Bitcoin as a virtual currency. The People's Bank of China has classified Bitcoin as something that is "not originally a currency, but an investment". A German court characterized Bitcoin as a unit of measure. The

[2]Open source software with a license to modify, modify and improve.

Finnish government, as well as Wall-Street, daily newspapers, have classified Bitcoin as a commodity. Bitcoin.org, the wiki portal for Bitcoin, gave the following definition: "Bitcoin is a payment method based on the concept of digital cryptocurrency, which functions without any central authority or third party as a creditor."[6]

As can be seen, the definitions differ significantly with regard to the aspect of observation. However, what is certainly an indisputable fact is that Bitcoin is a new technology or, more precisely, a protocol, and that any other function that Bitcoin performs derives from its technical characteristics as a protocol. Generally speaking, a protocol is an agreed procedure or set of agreed instructions to be followed in a given situation.

This cryptocurrency is not based on a gold base, is not tied to any country of origin and is not backed by any country, nor the Central Bank of a country, nor the Central Bank of a union of states. Thus, Bitcoin is the first cryptocurrency, i.e. the first form of virtual, digital currency that functions on the basis of cryptographic algorithms. Its basic characteristic is that there is no central authority, nor any central institution like the Central Bank, nor any other intermediary that manages it. There is the Bitcoin protocol, which uses Blockchain technology as support to achieve a fully decentralized system.

How does Bitcoin work? That is a question that is not very easy to answer. That answer is not so important for the functioning of Bitcoin itself as it is important for the explanation of the Blockchain technology, which makes it possible, which will be discussed in the next chapter. More important than anything for the functioning of Bitcoin is that a new user can start using Bitcoin without understanding the technical details of its functioning, in the same way that anyone can use the program without being its author or programmer. It is only necessary to install the Bitcoin Wallet application on a computer or mobile phone, which will then generate the user's Bitcoin address, that is, its account. Transferring Bitcoin from one address to another, or in banking terms "from one account to another", is in practice similar to sending and receiving e-mails. Just as in the case of e-mail, the sending user needs to know the address of the user to whom he is sending (the address of the recipient) a document or message, that is, a certain amount of Bitcoin, so he (the recipient) needs to know the address of the user who is sending it to him (the sender), if he wants to send something.

New cryptocurrency units are produced [7] ("printed") or, in banking terms, "emitted" by mining, as a reward for solving a mathematical task, set by the Bitcoin protocol, which verifies the newly created block and writes it into the Bitcoin Blockchain file, which will be discussed in more detail later in the text. Users can acquire cryptocurrency by purchasing a certain amount of cryptocurrency, and by selling goods or services. On average, a new block is generated on the Bitcoin Blockchain file every 10 minutes, so this is also the average time for transaction confirmation. After generating a new block, the

miner receives a reward (incentive) which currently amounts to 3,125 BTC (from 6,25 BTC per mined block to 3,125 BTC and which is halved every 4 years (BTC is the abbreviation for the Bitcoin cryptocurrency unit) as well as fees for transactions written in the new block. Mining is the only way in which new BTCs are "issued". The Bitcoin protocol defines the maximum number of Bitcoin cryptocurrency units, so it is one of the the reason why we can say that Bitcoin is in fact a deflationary currency. This is another difference compared to classic currencies, which central banks can issue as needed and in this way cause inflation. Until today it is"mined" or "issued" 19.746.787 BTC or about 94% of the projected sum of BTCs (21.000.000, and the current value (29.8.2024) of 1 BTC is 107.103,89 BAM.[8]

The more BTC there are, the smaller and smaller the reward, thus further preventing inflation. When miners have created 21 million bitcoins, this reward will be zero, and miners will only earn from transactions.

When we talk about Bitcoin transactions, we mean the transfer of money, or the value it represents, from one digital wallet to another, which is then registered as one digital record in the BitcoinBlockchain file (or the public ledger of all transactions), which together with other records (transactions) from all over the world, previously written in one block of transactions, is a block of still unconfirmed transactions. When all transactions generated within an average of 10 minutes from the moment of writing the last verified block into the BitcoinBlockchain file are collected, all miners are given the task to find the corresponding number, i.e. solve the corresponding mathematical problem. The first to do so ("wins the lottery") writes a new block of unconfirmed transactions into the BitcoinBlockchain file according to the system of chained blocks, so that from that moment all transactions in that block become valid and public. The size of that file today, 29.8.2024, has risen to about 596,51 GB[9].

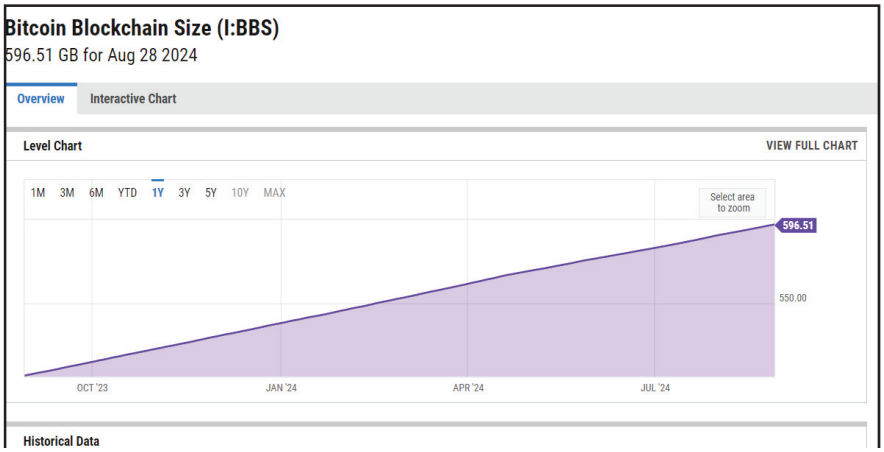


Figure 1. Bitcoin Blockchain file size[9]

A Bitcoin wallet contains a piece of data that is hidden from the public and is called a private key or password (the access code to the safe where the money is stored or the access code to the wallet). It is used to sign transactions confirming the mathematical proof that connects the key and the owner of the wallet. Once a transaction has been initiated and signed, it cannot be changed any more, which is exactly why the signature plays an important role. Transactions on the Blockchain network are public, and you can see the entire history (archive) of all processed transactions from the first to the last.

In practice, if entity A wants to send a certain amount of Bitcoin to entity B, it must have a digital wallet that contains a private key, which allows the creation of a cryptographic (digital) signature. Entity A enters the amount of Bitcoin that it wants to send to entity B. Entity B gives the public key (digital wallet address) to entity A to transfer the specified amount.

To be able to transact a certain amount of Bitcoin from one digital wallet to another, three things are required:

1. Wallet address or Public Key,
2. Privatekey or code access to the wallet and
3. Cryptographic (digital) signature.

When we describe the Bitcoin protocol, we often attribute two qualities to it: 1. that it is completely transparent (with a public balance book) and 2. that it is anonymous. If we focus on one item of the public balance book and the minimum necessary attributes for it to be recorded, we will notice that data such as name and surname, and other personal data are not necessary for the functioning of the balance book in terms of functionality, of course not taking into account KYC (Know Your Client) protocols, i.e. "get to know your client", which the bank must implement. The account number uniquely identifies the user, as is the case with the Unique Identification Number of the citizen[3] on the identification documents of the citizens of Bosnia and Herzegovina. That's why, when creating an "account" with the Bitcoin protocol, unlike creating a bank account, the Bitcoin protocol never requires the user to enter personal data. So, since this is a Bitcoin protocol, and not a bank, it would be more correct to use the term address, rather than account, as a label for the location where the number, which represents the amount of Bitcoin, is stored.

Every transaction in the Bitcoin protocol is public, and everyone has access to the public balance book, which they can see on the Internet at any time, as well as the history (archive or traffic) of all transactions made at any time from every active account.

Since the addresses of the participants in the transaction are not linked to their personal data, it is very difficult (practically impossible, but theoretically

[3]This number uniquely identifies every citizen of Bosnia and Herzegovina.

possible) to figure out which adress belongs to whom. This further means that Bitcoin is not anonymous, but a pseudo-anonymous system. However, we should not forget that everyone in the Bitcoin protocol can have an almost unlimited number of addresses.

The address is defined as a bank account. A Bitcoin address is an identifier 26-34 alphanumeric characters long, starting with the number 1 or 3, that represents a possible destination to pay Bitcoins using a cryptocurrency exchange account or through a digital wallet. It is important to point out that one user, as in the case of a bank account, can have and use several addresses.The example of Bitcoin address: 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY. These addresses are created using cryptographic algorithms, more specifically SHA-256[4] for generating private keys and RIPE-MD160[5] for generating addresses based on SHA-256 operation.

The private key is a unique and secret access code, which provides the right to transfer Bitcoins from the wallet using a cryptographic (digital) signature. When a new Bitcoin address is created, it comes with a private key that is mathematically linked to that account number. Bitcoin private keys usually contain 51 characters and start with the number 5. These private keys are memorized (stored) on a personal computer. In the case of using a software or web wallet, they are stored on the server.

A cryptographic (digital) signature is a mathematical method (algorithm), which is used to verify the origin and determine the integrity of information, and thus enables the owner to prove their ownership of a certain address, or wallet. Digital signatures have two essential characteristics:

- They ensure the integrity of the transaction (document), that is, they confirm that the transaction (document) has not been changed in the intermediate phase between reading (reviewing) and signing, and in the case of a contract that the articles and conditions have not been changed without the consent of both parties.
- The impossibility of forging a signature, which means that the signature uniquely identifies the signatory, and implies that it is not possible to avoid responsibility for the signed transaction (document), claiming otherwise.

At the moment when the Bitcoin protocol (software) signs the transaction with the corresponding private key, everyone in the Bitcoin network is enabled to display the (digital) signature that corresponds to the executed transaction and which is generated by a cryptographic algorithm, but the private key, which protects the account, is impossible to reach.

[4]The name of the algorithm for generating a digest (hash) from an input of arbitrary length, which will represent the private key.

[5]The name of the algorithm for generating a digest (hash), from an input of arbitrary length, which will represent a Bitcoin address.

A cryptographic hash function takes input data, i.e. a message or any string of characters of arbitrary length and converts it into a string of fixed length, i.e. an "encrypted" message better known as hash-code, hash-result, hash-value or simply hash[6]. This procedure is called hashing and is usually done using the Sha256 algorithm[7]. It is almost impossible to discover the original data from such an encrypted message. With the slightest changes to the input data to the hash function, the hash value changes completely.

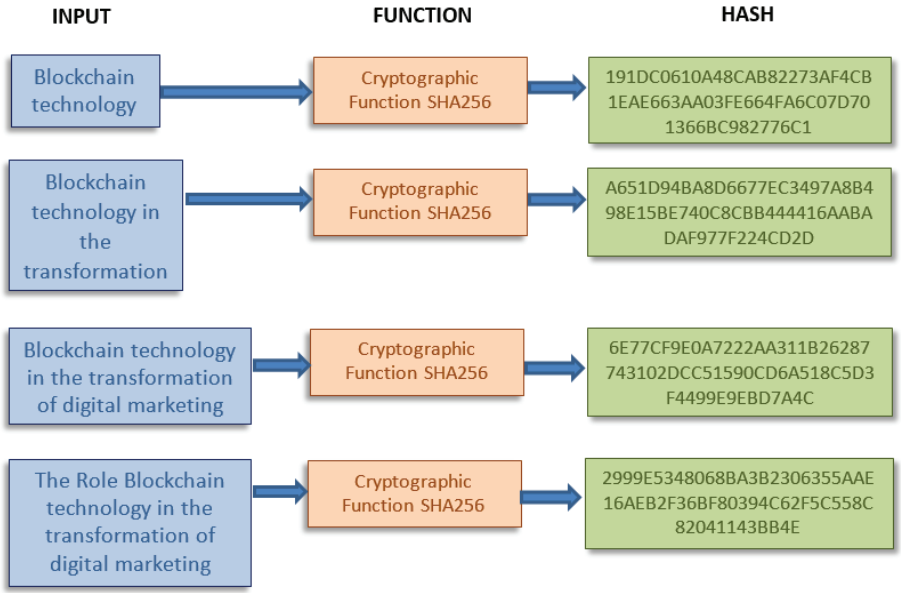


Figure 2. Calculating Hash Function Values for Different Inputs

2. What Is Blockchain Technology?

Most people still equate Bitcoin with Blockchain technology, so even though they are related, they are still two different concepts. The first practical realization of Blockchain technology was Bitcoin. We can say it differently. In order to realize the idea of anonymous digital money in the form of a cryptocurrency, it was necessary to find a new technology that would enable the decentralization of the management of that currency and the best possible

[6]A hash function is any function that can be used to map (convert) input digital data of arbitrary size to an array of digital data of fixed size (hash value). A good hash function is one in which small differences in the input data result in very large differences in the output data. Hashing is the process of obtaining a hash value.

[7]Hashing is the process of transforming an input of arbitrary length and obtaining a hash value of a fixed length, which in the case of applying the SHA-2 algorithm (Security Hashing Algorithm version 2) is 256 bits or 32 bytes or 64 hexadecimal characters.

protection of transactions. This is how Blockchain technology was born, which was quickly realized that it can be used for many other things, not only for the functioning of cryptocurrencies.

One of the basic ideas on which the concept of this technology is based is taken from accounting [7], and refers to the recording and archiving of all business transactions that have occurred since the establishment of a company. According to the principles of double-entry bookkeeping, every business event in the company is recorded so that the corresponding account is debited (increased), and another account or more are approved (reduced) in total for the same amount of the transaction or vice versa. Up-to-date records of all changes in accounting accounts (transactions) and the balance of these accounts are kept in a record called the general ledger or balance book.

What in the accounting records of the company is the main ledger with all transactions (changes) in all accounts of the general ledger since the beginning of the year, in the Blockchain records is the main Blockchain file, with all transactions since the beginning of record keeping.Records of transactions, i.e. changes in the accounts of the company's general ledger are kept in one place (the company's computer) and there is no verification of transactions by third parties, and the Blockchain record of addresses (user accounts) together with the transactions related to them, is kept in a large number places, that is, on powerful computers - servers around the world, which participate in the verification of each transaction and receive an appropriate reward for it. In the first case, when it comes to records maintained by the company, it is the main balance book, and in the second case, when it comes to Blockchain records, it is a public (global) balance book.

In the first case, since it is about central records or records in one place (computer), it is possible to change (maliciously or not) the content of transactions in a relatively easy way, whether it is done by company employees or someone outside the company who has access to this data via the internet. In the second case, it can be claimed with a very high degree of probability that this record is practically immutable, because it is kept in the same form on a large number of computers around the world, so in case of manipulation (hacking) attempts, it should be changed on all these computers, which makes it practically impossible. This is the second basic idea on which Blockchain technology rests, which could not be realized before the advent of the Internet and Peer to Peer computer networks (decentralized networks). The realization of this idea was also contributed to by the rapid development of hardware through an increase in the speed of the processor, an increase in the capacity and speed of access to external memory media, as well as the lower prices of the processor, as well as the main and external memory elements.

The third basic, and possibly the most important idea on which Blockchain technology is based, is the creation of additional security for

uninterrupted transactions, which is reflected in the impossibility of changing the content of once recorded transactions in the Blockchain file. The realization of this idea is done by connecting the blocks of transactions into a chain of transactions (Blockchain) in such a way that in each block of transactions, which is currently entered into the Blockchain, the content code (summary or hash) of the previously entered block is also entered, so if someone tries to change at least one character in any transaction block, the content code (hash) of that transaction block is also changed so that in that case it does not match the content code (hash) of the previously entered transaction block, and it should also be changed and so on until of the last written block. In other words, if someone wants to change the content of a transaction without authorization, he should change the hashes of all blocks from the block he wants to change to the last written block in the Blockchain file, and then distribute the changed file to all servers (nodes) around the world, which seems practically impossible.

Blockchain[10] represents a shared data structure, i.e. a list of information shared (distributed) between all nodes (nodes or servers) that are in the system (network). Given that the database is not stored in one place or on one server, it is decentralized. As the council has said more than once, decentralization, i.e. eliminating the need for the existence of a central authority, is one of the most important ideas of Blockchain technology. Instead of everyone who is engaged in some business and who generates some transactions in connection with it, having their own separate transaction record books, Blockchain technology offers them a unique and global (comprehensive) balance book, which contains all transactions since the beginning of record keeping, is public and is owned by all. It was created by the implementation of a Peer-to-Peer (P2P) network and a network of distributed servers (nodes), which mark transactions with a time stamp.

A Blockchain file consists of blocks, and each block can record a certain number of transactions, and a certain amount of data in a transaction. When a block is filled with transactions, a new one is created, thus creating an unbroken chain of interconnected blocks. When someone initiates a transaction from one address (account) to another address (account), it is time-stamped and recorded by every participant in the system), i.e. owned, because the balance of the account is public, synchronized with other system participants and transaction records, and the rules are defined at the beginning and implemented through program code. In this way, double spending problem[8]was solved without third parties, i.e. an intermediary trusted by both parties.

Blockchain is based on a distributed database, which eliminates the need for a separate entity (bank, state, municipality, court, lawyer, notary,

[8]The possibility of spending the same (virtual) money effectively at least twice, because it is recorded in digital form.

intermediary marketing agency, etc.) that will manage transactions as an intermediary and ensure the security of their performance. Thus, one central register of transactions with all transactions since the beginning of record keeping in the centralized banking system is replaced by copies of Blockchain files on a large number of powerful computers (servers), which will be located in different locations, which are called nodes. The owner of these powerful servers can be anyone, that is, anyone who applies for such a job and provides the availability and possibility of updating the records (Blockchain file) to all participants in the transaction at any time of the day. Due to the fact that this job requires significant investments in equipment, as well as the payment of electricity, computer administration and maintenance costs, it is logical that none of the participants in the transaction will apply for such a job just like that. In order for someone to engage in these jobs, there must be an appropriate reward for entering and doing such work. The basic task of "miners" is to confirm the transactions of the participants in the transaction and to ensure their validity.

Systems that use Blockchain technology belong to peer systems (Peer-to-Peer) and are called decentralized or distributed systems. In this way, the exchange of data through the computer network is enabled, whereby the nodes receive information from each other instead of from one central computer. With respect to the tasks that equal partners can perform, there are four types of partners. These are: a simple partner or a partner called a "simple wallet", a "router" partner, which performs network routing, a "miner" partner, which performs mining, i.e. finding the code that closes the block transaction and maintenance of the entire Blockchain. In a private Blockchain system, each partner manages all four tasks.

3. Application of Blockchain Technology in Digital Marketing (Blockchain Marketing)

An example of a P2P network is represented by torrents such as the BitTorrent[9] client, on which model Bitcoin was constructed. The first software application that used a P2P network was called Napster. It was launched in 1999, and was used for sharing primarily audio and video, but also other content. Napster made it possible to search for content, and often illegally "download" of mentioned content. Napster is an application, which was still partially centralized even though it relied on a distributed P2P network. Let's assume that a Napster client is installed on each of the several thousand computers that make up the network.

[9]BitTorrent is just one of the tools in a series that helps to share data more easily and quickly, unlike the conventional ways of sharing data via a centralized server, via email or File Transaction Protocol (FTP). While, for example, email and FTP rely on a central hosting server and sending data to connected computers, BitTorrent relies on a network of users where everyone sends data to everyone (peer-to-peer network).

When someone (peer1) using one of those computers wants to "download" some video content in the form of an mp4 file, it is necessary to connect to the Napster server. This server performs the role of an intermediary and its sole purpose is to index the contents of other computers in the network and inform the owner of the computer (peer1) about other computers in the network that are online and have the requested content on their hard drives. The job of this server is not to store store the requested content (file), but to provide a service of referencing that content in the network and help in establishing a connection between these points (computers) in the network.

In this sense, the server can be described as a central indexing server. This is the reason why P2P networks are often in the "grey zone" of the law, precisely because they have no direct contact with potential illegal files, nor a way (technique) to control the freedom of users to "download" the content they want. This partial centralization in the form of a central server for indexing was a weak link in the Napster system, so it is abandoned, and the BitTorrent protocol, designed by Bram Cohen, enters the scene.

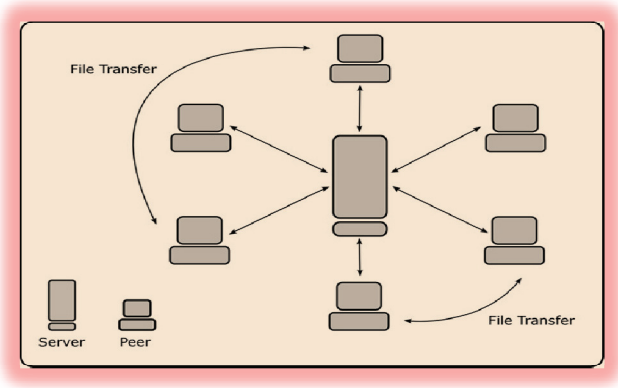


Figure 3: Napster server architecture configuration [11]

When it comes to Blockchain digital marketing, the most important are three changes, that is, differences in relation to not only traditional, but also digital marketing, which could revolutionize marketing as we know it so far. Namely, it is about the potential inherent in Blockchain technology and which enable the removal of the digital intermediary, increasing transparency and giving consumers back control over the sharing of their own data. [11].

As we have already emphasized in the paper, the Blockchain did experience its first application by enabling the functioning of the first cryptocurrency Bitcoin, so this is the main reason for the initial connection of this technology to Bitcoin, but it is clear to everyone today that the Blockchain is

much more than Bitcoin itself and that it has a huge the potential of application to all areas of human activity, not only cryptocurrencies.

One of the main areas where the application of Blockchain can make radical changes is digital marketing. One of the most important aspects of Blockchain technology is enabling decentralized, i.e. direct communication between different parties in such a way that every detail of that communication is verified and documented.[11]

The first change brought by Blockchain Marketing compared to traditional, i.e. digital, marketing is the ability to completely eliminate the intermediary in digital marketing.Digital marketing uses „intermediaries" which control the space between the advertiser and the user. Take, for example, Search Engine Marketing (SEM)[10]. One of the reasons a website chooses to display Google banner ads on its site, as opposed to organic finder advertisers, is that Google is a trusted source. If the company was „reviewed" Google Display Network, then it's likely to be a credible business that won't damage the host site's brand. Google also performs transaction processing so that the website owner is paid fairly for the clicks generated on the advertiser's ad. In this case, Google is basically an intermediary between the advertiser and the website owner. For this reason, they reduce profits.

Now imagine SEM through the Blockchain. Website owners would not have to go through the Google Display Network to find advertisers, as each „user" had already been confirmed and authenticated. The advertiser would know they are paying for real clicks and the website owner can trust that the amount they are being paid is fair. There would be no need for Google (or Facebook or any other intermediary). It all comes down to reducing additional costs and increasing the profit margin.

The second change [11]brought by Blockchain Marketing compared to traditional, i.e. digital marketing is the increase in transparency between advertisers and users, which builds and increases trust between them. One of the frequent problems faced by many companies, mostly large ones, is the problem of consumer trust. Customers are suspicious of everything they buy, from the origin of the food they buy to the factory conditions in which the clothes they buy are made. Companies gain customer trust with the help of transparency, which Blockchain marketing can provide in a way that some other tactics and techniques cannot. An additional advantage and value of Blockchain marketing is the level to which everything is documented and verified. For example, with the help of Blockchain marketing, a customer could find out the "behind the scenes" view of the seller's supply chain, i.e. get accurate information about how

[10]Search Engine Marketing (SEM) is the process of generating traffic on a website by purchasing advertisements on internet search engines. For many users, the journey from obtaining information about a product to purchasing a product begins on Internet browsers. They get the answer to every question by searching through an internet browser.

the product is made. Transparency allows the consumer to find out whether the company is telling the truth when it publicly presents its products or not, whether it is trustworthy or not.In one case study, Walmart hired IBM to create a project that aims to make their supply chain process as transparent as possible. By digitally searching the chain blocks that store information about the origin of their products, consumers have been given the proof they need to trust what Walmart is selling them.

The third change brought by Blockchain Marketing [11]in relation to traditional, i.e. digital marketing is enabling the consumer (user/buyer) to control the sharing of their own data. Blockchain Marketing has the potential to find a way in the future to balance advertising with consumer identity issues, i.e. how to not violate consumer privacy through advertising."There are already several services that offer the user full control over their identity and transaction history, such as uPort, MetaMask and Keybase. This means that marketers will have to earn the customer's permission in a way that is completely different than before: Blockchain allows consumers to pay attention to their contact information. In the future, the advertiser may end up paying the user to consume their advertising material."[11]

In addition to these three changes for which Blockchain Marketing has the potential, some other advantages that it has compared to traditional marketing should be mentioned. They are[12]:

1. **Blockchain has the potential to drive public responsibility**, i.e. socially responsible business. Transparency and documentation stored in Blockchain files can be used to create digitized contracts that can be viewed by the public and used to pressure companies to be socially responsible.

2. **Blockchain has the potential to offer advantages for easier and better branding.** If the company uses innovative technologies, such as Bitcoin-friendly payment methods and/or the use of Blockchain to formalize digital negotiations between companies, it will be seen as an advanced and robust organization. In other words, Blockchain Marketing increases transparency and trust in the brand. "For example, if a business used Blockchain to track the delivery of a purchase and allow both parties (both buyer and seller) to see where the package is on its journey, this increases consumer confidence in the business to deliver the item. This represents a leading USP[11] for marketing companies for promotion and a means of attracting more market share"[12].

[11]It is a specific advantage that the seller has compared to the competition, which tells the buyer how the seller differs from the competition and why he should choose him.

3. Blockchain technology opens international markets. The first way Blockchain can benefit digital marketers takes us back to its most famous use - cryptocurrency. If marketing efforts can include and promote the use of cryptocurrencies to purchase products and services using online Bitcoin wallets, it opens up an international market. This happens because cryptocurrency payments can be made across borders without additional fees. This will motivate more people to buy from overseas companies and this is something that retailers can use to their advantage. [12]

4. Blockchain helps in handling Big Data[12]The potential relationship between Big Data and Blockchain has not been fully explored. It is predicted that Big Data could analyze the Bitcoin Blockchain to detect trends and help understand price fluctuations, as well as predict the future value of Bitcoin. Another benefit though, is that large amounts of data can be stored on Blockchain files to keep the records secure and unaltered, preventing them from being lost and helping to improve the accuracy of big data analysis between large teams. There is no reason why this cannot be the case with marketing departments as well. A large marketing team may want to analyze consumer trends from a dataset, and by keeping that data within an internal Blockchain, team members can work more efficiently without multiple versions of the same dataset. This will overall increase the accuracy of the final result and prevent data loss.

The greatest impact of Blockchain technology is reflected in the area of leasing advertising space on digital channels. To a lesser extent, Blockchain technology affects the value of data that customers/clients/users continuously leave on the Internet, and in connection with that, the way of communicating through digital channels, i.e. the creativity of the message. Not so long ago, and even today, one of the biggest challenges in the field of digital advertising was security, i.e. lack of trust, and the impossibility of checking the accuracy of the information received. This is most pronounced with programmable advertising, i.e. renting digital advertising space with the help of innovative technologies and advanced algorithms.[13]

Programmable platforms are mediators between advertisers and media that, with the help of advanced technology, provide the advertiser with the highest return on investment. The programmable platform provides the possibility for advertisers to find targeted groups of users in the right place at the right time on online channels and to communicate the right message to them. The key problem that arises here is non-transparency, which results in the

expansion of the space for fraud. "One of the most famous and biggest cases of fraud in digital advertising is the so-called "Methbot Fraud". Namely, Russian hackers created a network of fake portals with a name similar to CNN or FOX. They made them so well that they managed to deceive the ad networks that, due to wrong recognition, placed ads on them from some of the world's biggest advertisers. At the same time, they developed a bot that could simulate human behavior and click on those ads. In this way, they earned over 180 million dollars. Thus, the advertisers paid 180 million dollars for clicks on ads that no one ever saw, and the portals were left without 180 million dollars in income because these ads were not shown at all".[13]

The creators of Blockchain solutions made sure that such things would not happen in the future. A new layer has been added to the intermediary, that is, the programmable platform, which enables a more significant level of transparency, and eliminates the space for malfeasance and fraud. Every click, every payment and display is recorded in a Blockchain file, so that record cannot be deleted or changed. This record is available and clearly visible to everyone at any time. One of the better examples of Blockchain platforms that try to take the programmable mechanism to the next level with the help of Blockchain technology is AdBank network. [13]

4. Conclusion

Due to the potential and benefits provided by the application of Blockchain technology, which are reflected in the provision of transparency, the availability of accurate information and the verifiability of the accuracy of this information, the practical impossibility of erasing and changing information once recorded, the elimination of almost all fraud and malfeasance, the elimination of all intermediaries in any processes, it is expedient and advisable to use Blockchain technology in marketing. One of the most significant benefits of using Blockchain technology is to give consumers back control over their personal data, eliminating the possibility of companies taking unauthorized data from customers (in a way that seems to be taken for granted) without offering them any compensation for it. As emphasized in the abstract of the work, the goal of this work was to point out the incredible, that is, the revolutionary potential of Blockchain technology in almost all areas, including in the field of Marketing. What could be concluded when it comes to the application of Blockchain technology in Marketing or Blockchain Marketing is that it puts customers in a significantly more favorable position, primarily because they have the option of checking the accuracy of the information that advertisers place on them, both in relation to the origin of the product , as well as with the entire product supply chain, which prevents abuses and eliminates fraud. The following benefits provided to customers by Blockchain Marketing are the

possibility to pay for products with cryptocurrencies, then the possibility that before purchasing the product, customers have all the relevant and true information about the origin of the product they are buying, and the change in the paradigm of ownership, i.e. control of their personal data, which is returned to them, and also they can earn extra money from it. As for the benefits for merchants, Blockchain Marketing provides them with direct access to customers without intermediaries such as Google, Facebook, Amazon, and in this way ensures a better quality of communication with customers, as well as a reduction or complete elimination of advertising costs through intermediaries, etc.

As a consequence of the application of Blockchain technology in marketing, the concept of data ownership is changing. Facebook changed the well-known slogan "data is the new gold" to "we enable you to use the software platform for your needs, and in return we get your data that we will use for our needs". [13]Blockchain technology offers the potential to change the paradigm of data ownership in this area as well. So there are already media and platforms that are ready to pay for the time that customers spent reading ads, as well as the data that customers gave them.

4. References

[1] Chaum, D., *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.* Caliornia University, Department of Computer Science, 1981.

[2] Chaum, D. (1982). *Blind Signatures for Untraceable Payments.* Caliornia University, Department of Computer Science, 1982.

[3] Zimmermann, Ph., *PGP Source Code and Internals*, ISBN 0-262-24039-4.MIT Press, 1995.

[4] Hughes, E., *A Cypherpunk's Manifesto,* Nakamoto Institute, 1993. https://cdn.nakamotoinstitute.org/docs/cypherpunk-manifesto.txt [Accesed:13. 01. 2019]

[5] Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcion.org, 2008. https://bitcoin.org/bitcoin.pdf [Accesed:13. 01. 2019]

[6] Stupar, S., Bičo Ćar, M. Šahić, E.“*Challenges of Applying Blockchain Technology*”. In: New Technologies, Development and Application II. NT 2019. Lecture Notes in Networks and Systems, vol 76. edited by Isak Karabegović. Springer, Cham. 2019.

[7] Stupar, S.,“*Blockchain - Tehnologija bliske budućnosti?*” u Zbornik radova Jahorina Business Forum - VIII naučna konferencija, 339-348, Jahorina, mart 2019.

[8] Kripto.ba, *Bitcoin,* 2019. https://kripto.ba/bitcoin/, [Accesed: 29. 08. 2024]

[9] Ycharts, *BitcoinBlockchain Size*: *Daily report and Interactiv Chart*; Ycharts, 2024.

https://ycharts.com/indicators/bitcoin_blockchain_size[Accesed: 29. 08. 2024]
[10] Gupta, M., *Blockchain for Dummies*, IBM, John Wiley & Sons, Inc., Hoboken, New York, 2017.
[11] Siu, E., *Chapter 2: What is Blockchain Digital Marketing*; Single Grain, s.a., https://www.singlegrain.com/blockchain/blockchain-digital-marketing-101/ [Accesed: 29. 08. 2024]
[12] Gem, F., *The impact of blockchain in digital marketing*, Media Update, 2020. https://www.mediaupdate.co.za/marketing/147788/the-impact-of-blockchain-in-digital-marketing[Accesed: 29. 08. 2024]
[13] Drmač, D., *Kakoćeblockchainuticatinadigitalni marketing*; Marketing mreža, s.a.https://marketingmreza.rs/kako-ce-blockchain-uticati-na-digitalni-marketing/ [Accesed: 29. 08.2024]