MANAS Journal of Engineering
ISSN 1694-7398 | e-ISSN 1694-7398

Volume 10, Issue 1, (2022) Pages 60-65
https://doi.org/10.51354/mjen. 1034912

A glance at blockchain technology and cryptocurrencies as an application

Turgut Hanoymak[1,*], Ömer Küsmüş[2]

[1] Van Yüzüncü Yıl University, Van, Turkey, hturgut@yyu.edu.tr, ORCID: 0000-0002-3822-2202
[2] Van Yüzüncü Yıl University, Van, Turkey, omerkusmus@yyu.edu.tr, ORCID: 0000-0001-7397-0735

ABSTRACT

Blockchain technology, which includes cryptocurrencies such as Bitcoin, Ethereum, etc. [1,2] which has been evaluated as an investment tool by many people all over the world in recent years, needs to be examined in detail, both mathematically and conceptually [8,9]. In fact, it can be said that blockchain technology, which is characterized as an accounting system and database based on distributed ledgers in its most basic form, is extremely secure in terms of attacking. For this reason, we can say that technology has a more effective security mechanism than any central state-of-the-art authoritative system used today. However, as it is almost impossible to bring all of the security, speed and cost parameters to their full extent in a system at the same time, as in any cryptosystem, the security parameter from the distributed ledger structure in blockchain technology adversely affects the speed and cost parameters. In this article, we discuss the cryptographic working principles of cryptocurrencies, which is an application field of blockchain technology, together with blockchain technology and the features and structures of the blocks contained.

ARTICLE INFO

Research article

Received: 9.12.2021
Accepted: 20.02.2022

Keywords:
Blockchain,
cryptocurrency,
bitcoin,
ethereum,
distributed ledger,
decentralized

*Corresponding author

1 Introduction

Bitcoin, a financial instrument that almost everyone has been talking about recently, has attracted attention with its performance. Bitcoin and the technology of blockchain, which is the infrastructure of bitcoin, has become one of the most curious subjects of today due to its deflationary structure. Some people think that bitcoin is a pyramid scheme because it is illegal and virtual. However, others describe bitcoin and blockchain as the revolution of the future that affects almost everything, as both financial and social. As a result, some views regarding this technology have existed for a long time. Because of these two opposing views, it is possible for people to understand the essence of this technology only if the subject is studied by experts and the right information is transferred to people. Otherwise, people may continue to fall into financial difficulties by acting with the approach and advice of some malicious people due to the dark spots of this technology. People who are exposed to this situation also think that the technology is a fraud instead of protecting themselves from these malicious people. In our point of view, the people who have an interest in this technology should firstly read and study to have a technical understanding of its basics [3-8].

Blockchain technology was delivered to people in 2008 by an anonymous person or group of people named Satoshi Nakamoto with an article called Bitcoin written in academic language [1]. Understanding and adopting the essence of the business in the early days was really difficult for experts. This technological idea, which came to our minds with this theoretical article in 2008, started to become a financial instrument in 2009.

In order for people to understand why these developments actually took place in those years, they should closely follow the economic events that took place in the world at that time. The economic crisis, which started especially in the USA in 2008 and emerged as a result of an inflationary policy, caused people all over the world to question their management styles and seriously undermined the confidence in the financial policies of governments [11,12].

After this financial crisis, the concept of collateralized debt obligation began to be discussed and understood in society. Satoshi Nakamoto suggested that bitcoin should be seen as an alternative payment and exchange tool, not a derived money, in his article, which he published believing that the deflationary nature of money would protect societies from this crisis as a way to prevent such crises due to inflation. Thus,

for the first time in history, a definition of money, which was not under the control of the states and was a product of common intelligence, naturally aroused the reaction of the state authorities. Of course, bitcoin would not be like a commodity, a stock, or a fiat currency. The biggest criticism of governments for cryptocurrencies is that it is almost impossible to follow the transfer processes of cryptocurrencies and the potential of cryptocurrencies to be served for illegal groups or actions due to this following problem of cryptocurrencies. We actually do not think that cryptocurrencies have a tracking problem because, investigating the blockchain where the transfers are recorded, transactions in each block appear transparently with addresses specified in hexadecimal numbers. As a result of a rigorous criminal investigation, the state security forces can find out who these addresses belong to. In other words, it is very easy to follow the account numbers of the transactions made. However, at that time, it is not possible to track who have the accounts. Due to this feature, the ability of bitcoin to be used for money laundering and the underground economy is still a huge disgrace. The website Silkroad was founded in 2011 and was shut down twice in 2013 and 2014. On this site, it was possible to find illegal products such as various drugs, weapons, hired killers, credit card copying and child pornography. Bitcoin was used to pay for these illegal transactions on the site. However, it is argued that must emphasize that it is the business itself to be blamed here, not the use of bitcoin as the same accusations can be done for governmental printed money.

In terms of its working principle, in general, bitcoin or cryptocurrencies is a financial product based on blockchain technology, which aims to transfer money safely and quickly between two parties without any intermediary [12]. In the following sections, the structure of the blocks of the blockchain will be discussed in detail. However, to explain briefly now, it can be noticed that in order to ensure the security of this intended money transfer, the transactions must be recorded with more than one record holder. However, we realize that these transfer transactions, which are intended to be made quickly by peer-to-peer with a very low commission fee, contradict the genesis purpose of bitcoin due to problems such as the increase in commission fees and the prolongation of transfer times in recent years. Therefore, the technological solution proposal for each of the current problems of blockchain technology, called scalability, introduces new cryptocurrencies called alternative coins (altcoins).

As mentioned before, the biggest financial problem of current cryptocurrencies in the blockchain and the biggest obstacle to their use as a payment tool is the scalability problem which can be defined as slowness of transactions and high transaction fee.

2. The structure of blocks in a blockchain

In this section, we mention the mathematical structure of blocks in a blockchain. As mentioned in the previous section, we recall that blockchain technology is basically a database and this database is a technology with a distributed ledger structure. Data can be stored sequentially in blocks, and each block has a timestamp indicating when transactions are made. As the blocks fill their capacity, the next blocks are opened and the data starts to be recorded in this block. Each blockchain has some peculiarities of its own. With these features, the size (capacity) of the blocks contained in the blockchain and the information fields of the blocks (title, password, timestamp, version number, fingerprint of each record and the protocol to which it belongs) are determined. In every blockchain, it is necessary to know the structure of the blockchain in order to determine the way records are saved, which fields they will contain, how they will be ordered, what happens when the block is full, the conditions for generating new blocks, the characteristics of inter-block connections, how the blockchain will be distributed in the network, stored and controlled. If these features of the blockchain are secure, practical and useful, it is expected that the interest and demand for that blockchain will be higher. In a blockchain, the most important factor required for this security, practicality and usability among users on the network is mathematical hash functions.

Hash functions are very useful tools in the field of cryptology. A hash function by itself is not an encryption algorithm. It is essentially more convenient to think of hash functions as tools which satisfy authenticity and integrity. It is used to test and prove the authenticity of a data, message, document. The Secure Hash Algorithm (SHA) is an algorithm that creates a fixed-length output no matter what data it is [13]. A slightest change in a document causes a big change in the hash value. Hash value is the output or image of an input under a hash function. Therefore, when the hash value of the original document is compared with the hash value of the document that reaches us, it becomes clear whether the document is original or not. So, hash functions are used to determine the authenticity of a document.

An algorithm is required for encryption and decryption operations. For this, mathematical hard problems such as Integer Factorization Problem (IFP) [14], RSA Problem [15], Discrete Logarithm Problem (DLP) [16] are necessary. Asymmetric encryption algorithms are the only algorithms that meet the needs of the information world today. Asymmetric encryption algorithms contain a private and a public key.

The two main concepts required for the security of all transactions on the blockchain are confidentiality and integrity. An effective encryption algorithm against all kinds of attacks is required for confidentiality, and hash functions

with some features are required for integrity. The most popular among cryptographic hash functions is the SHA series hash algorithms developed by NSA. SHA-0 (in 1993), SHA-1 (in 1995) and SHA-2 (in 2002) are some of them. However, the most common and still used hash algorithm is SHA-256, which is 256 bytes long. Ideal hash functions have five key properties:

1. The same input should always produce the same output (hash value).
2. The function should be able to be calculated very quickly.
3. Input cannot be calculated using output.
4. A small change on the message or input should be able to produce a very different hash value.
5. Different inputs should not produce the same result (collision-resistant).

A hash function with these properties is a key element used to connect blocks and ensure immunity. The hash of a block appears as the input of the next block. This provides a very protective effect in terms of preventing attacks on basically any block, due to the feature of the ideal hash functions in the 4th item described above. Because even the slightest attack on a block, that is, its hash input, will change the output. Since this changing output is the input value of the next block, the hash value of the next block will also change, and as a result of this attack, the hash value of all blocks will change iteratively. This is an attack process that can be detected instantly across the entire blockchain, and the probability of the attack being successful is negligible. The first block created in a blockchain is usually called the genesis block, and since the previous block does not exist, a 256-byte-long hash input consisting of only 0 is systematically assigned.

In a blockchain, each block has a parent block because it is created by the hash output of the previous block. Except for the Genesis block, each block has a unique parent block. However, a parent block has more than one child block. Now, we examine the structure of blocks, which are the bricks of a blockchain. A block consists of 4 basic areas. These areas are shown as follows:

Table 1. *The Areas of Blocks*

Field Name	Size	Context
Block Size	4 Byte	shows the size of the block
Title	80 Byte	consists of some fields
Counter	1-9 Byte	Display number of the operations
Records	Variable	Saved operations

Block size displays the total size of the operations which are realized in the block. Title consists of six subfields in itself. These subareas are given in the following table:

Table 2. *The Areas in the Title of a Block*

Field Names in Title	Size	Context
Version	4 Byte	follows updates
Hash of the previous block	32 Byte	hash value of the parent block
Hash of the Merkle root	32 Byte	hash value of the root of the Merkle tree in the block
Timestamp	4 Byte	construction time (seconds)
Difficulty Level	4 Byte	difficulty of proof of work (PoW)
Nonce	4 Byte	A counter for PoW

Version specifies which rules are valid in the relevant block of a blockchain. While creating a block, there are many rules to be followed such as its structure, length, record type, order of fields. One or more of these rules may be changed over time. Which blocks in the blockchain will be affected by this change and how will be determined by the version number.

The hash of the previous block is a key element which correlates the previous block with the next block. When a block is completed, its hash is generated. This hash is also one of the inputs for the next block. This feature ensures that the chain is unalterable, or in other words, protected against attacks. But that doesn't mean that blockchain registrants can't make the changes they want. The subject is directly related to the Merkle tree and the Merkle root.

Merkle root is actually a value obtained as a result of binary grouping of each transaction in the blockchain and calculating the hash values. The last value obtained as a result of these iterative operations by taking the hash is called Merkle root. Since transactions are hashed in pairs, if the number of records is odd, then the last record is hashed with itself. The reader who wants to better understand the Merkle tree and the Merkle root can refer to [17,18].

Timestamp indicates when a block was generated. It is displayed in Unix's epoch time format. This shows how many seconds have passed since January 1 1970, GMT 00:00. 4 bytes are reserved for the timestamp. This one is 32-bit. Since the first bit is reserved for the sign of the number (positive or negative), we have a 31-bit binary number. So the largest number that can be written is $2^{31} - 1 = 2147483647$.

The degree of difficulty is a concept directly related to the introduction of certain limitations and conditions on the hash value to be calculated. Even today's average computer is capable of calculating the hash value of a block in a short time.

It should be noted that finding the hash value of a block means creating that block. However, the blockchain system is programmed so that each block can be completed within 10 minutes. In other words, the computer does a job that finding the relevant hash value within 10 minutes. This is called mining by the miners in the blockchain. For example, the system identifies a problem when miners find an input whose first 40 bits are 0, and the miners try to be the first to complete the job. It is called Proof of Work (PoW) that the miner who completes the given job first is rewarded in the blockchain. If the time it takes to find these inputs, which we call the nonce value, in a way that meets the given conditions, that is, if the problem becomes more difficult, then an update is made on the timestamp of that blockchain.

Nonce is the generic name given to disposable numbers in computer language. In a blockchain, the difficulty level is based on finding the nonce value that meets the given conditions. The nonce discovery process by miners is essentially based on brute force. We now know that the time taken by this brute force operation varies directly with difficulty and timestamp. In PoW, miners compete with each other to be the first to find the nonce value. Recently, ethereum, which can be considered as the largest application of blockchains, uses PoS (Proof of Stake) method instead of PoW and develops an algorithm that adds smart contracts to the blockchain [19,20].

In PoS method, miners do not compete with each other using their computational power. Instead, each miner in the system has the right to be assigned the task of creating blocks according to his stake. In PoS method, miners collect their data in a pool and the next block creation task with this data is determined by a completely random function. However, the probability of a particular miner receiving this task is shaped by the help of this function and the stakes it has. One of the most distinctive features that distinguis PoS method from PoW method is that miners do not earn rewards after completing the block creation task in PoS method. He earns only commission fee based on his transactions. Another advantage of the PoS method over PoW method is the reduction of energy consumption, which is important for environmental health. In the PoS method, as in PoW method, each miner does not calculate for the nonce value. Since a selected person will do this calculation, there are direct energy savings. However, by the way, it should be noted that the selection of this single person in PoS method contradicts the distributed nature of the miners. This causes the task of creating blocks to be given to more stakeholders each time. It can be said that this is a contradiction in terms of centralization.

With all these advantages and disadvantages, we think that it is possible to prevent the block formation time, which is called the scalability problem of PoW or PoS method in the blockchain, which is still an open problem and cannot catch up with today's financial systems. In the next section, we will consider how blockchain can be used in finance and other business sectors when the scalability problem is solved.

3. Issues that will be affected by blockchain technology in the future

We now know that blockchain is a database where all records cannot be changed and only authorized persons can enter data within the framework of their authority and are kept in multiple copies in a distributed manner over the entire network. By placing smart contracts in this database, we can leave it entirely to the algorithm in which case what kind of ratio will be taken. There is no single center where all the data is collected due to the entire distributed storage of the database. Therefore, there is no such thing as a server crash, system hacking, malicious internal damage or deletion of data. It is also useless to destroy or replace a certain part of it, as losses are kept in multiple numbers. Because the terminals in the system have algorithms that check whether the records they have and other records are the same when using the blockchain. If two blockchains being compared to each other are different, the system queries which chain is present in the system. It discards the chain that is not in the system and continues processing the most common chain. All blocks in the blockchain are linked to each other by their hash values. The hash value of any block is one of the entries of the next block. Therefore, no matter which block is changed in the chain, the hash values of that block and all subsequent blocks change. This malicious terminal needs to calculate hash values of all communities one by one. The existing chain length of the system needs to be caught and crossed, which is unlikely. All records in the chain are stored sequentially. Recording or reading the chain is possible with passwords. In this way, data entry or data reading is provided at the depth of the chain, which is of interest to whomever. For example, the Bitcoin blockchain is an open chain. Anyone using a suitable application can read data from the system. In addition, anyone can enter data into the chain with appropriate applications using private key cryptography. Of course, this process is done within the framework of certain rules. However, for the blockchain that you will use, for example, in your shipping company, it is possible to set the read-only permissions and the data-write permissions and their depths. In our opinion, the most important feature of the blockchain, which we call the greatest invention after the establishment of the internet, is trust, which we say will cause great social, financial and legal changes. One of the most effective features of the blockchain is that the trading parties do not have to know and trust each other. It is possible to create such a platform without introducing a third party such as any central, notary, bank, referee, etc. The absence of a third party, that is, a centralized structure is very positive in terms of speed and cost of information confidentiality in transactions. Our general point of view on this issue is that the method of intermediary services and the institutions providing this service will either

disappear or undergo a structural transformation in the near future.

Banks that collect deposits from those with surplus resources and give loans to those in need, real estate agents who bring together those who want to sell their house and those who want to buy a house, an institution of notary public that witnesses any real estate purchase and sale and creates official records, letter of credit transactions that provide assurance in export and import, for example, intermediaries such as Swift, Western Union or MoneyGram that deliver the pocket money sent to a student studying abroad after 2 or 3 days or demand a high commission, security forces checking if a person is 18 years old, recruiters who had to check our manually prepared CV's during some job interviews, Music and art world people who want to protect their works from the pirate internet market, rental or logistics services, companies that provide hotel reservation services such as booking.com.

In short, the institutions, structures and services that provide brokerage services will change in the future. Moreover, blockchain technology may be used in electronic voting schemes such as the elections of governments by providing electronic and more secure systems. Blockchain technology promises to be quite a groundbreaking revolution such as printing presses, steam machines, airplanes, computers, the internet and e-mail have been in the past.

4. Conclusion and Discussion

In this article, we discuss blockchain technology, cryptocurrencies which is one of the applications of blockchains and their cryptological backgrounds such as private key cryptography, hash functions, etc. Also, we review technical informations about the structure of blocks in a blockchain and some items that the blocks and the header of a block carry.

In the end, we discuss which problems will be eliminated by blockchain technology and which problems of the companies that provide intermediary and brokerage services in social life will be facilitated in the future. We think that the glance at blockchain technology is like the glance at internet revolution in 1990s' Turkey for now. It still has many unknown features and many challenges or aspects to be applied for certain problems that need improvement. Unfortunately, due to its shortcomings, some abuses of blockchain technology, especially platforms in the cryptocurrency exchanges can be seen prominently against people. However, we think that states can prevent such abuses using constitutional regulations in capital markets laws. In this way, both cryptocurrencies and other applications of blockchain technology will provide more confidence to society being further integrated into the current financial system.

References

[1]. Nakamoto S., "Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf , May-2009 (Accessed on 20.07.2018).

[2]. Vitalik Buterin. Ethereum white paper, 2013. https://github.com/ethereum/wiki/wiki/White-Paper

[3]. Polvora A., "Blockchain Now and Tomorrow, European Commission", Joint Research Centre, Brussels – Belgium, 2019.

[4]. Çarkacıoğlu A., Kripto-para Bitcoin. Research Report, Capital Markets Board of Turkey, Research Department, December-2016.

[5]. Antonopoulos A.M., Mastering Bitcoin. 1st Edition, O'Reilly Media, Inc., December-2014.

[6]. Prypto, Bitcoin for Dummies, A Wiley Brand. John Wiley & Sons, Inc., ISBN-13: 978-1119076131, 2016.

[7]. Rykwalder E., The Math Behind Bitcoin. https://www.coindesk.com/math-behind-bitcoin/ October-2014 (Accessed on 20.07.2018).

[8]. Sert T., Sorularla Blockchain, Türkiye Bilişim Vakfı, 2019.

[9]. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies: A comprehensive introduction. 2016.

[10]. Bonneau J., Miller A., Clark J., Narayanan A., Kroll J.A., Felten E.W.. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In 2015 IEEE Symposium on Security and Privacy, 104{121, May 2015.

[11]. Williams, Mark. Uncontrolled Risk. McGraw-Hill Education. s. 213. ISBN 978-0-07-163829-6(2010).

[12]. Andreas M. Antonopoulos, 2014, "Mastering Bitcoin", O'Reilly, 330 s.

[13]. Preneel B., Cryptographic Hash Functions, European Transactions on Telecommunications, 5, (1994), 431-448.

[14]. Pomerance C., Factoring, Cryptology and Computational Number Theory, 42, Proceedings of Symposia in Applied Mathematics, 27–47, American Mathematical Society, 1990.

[15]. Rivest R.L., Shamir A., Adleman L.M., A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21 (1978), 120–126.

[16]. Mccurley K.S., The discrete logarithm problem", C. Pomerance, editor, Cryptology and Computational Number Theory, volume 42 of Proceedings of Symposia in Applied Mathematics, 49–74, American Mathematical Society, 1990.

[17]. Merkle R.C., "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[18]. Merkle R.C., A Certified Digital Signature, Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings.

[19]. Dwork, Cynthia; Naor, Moni "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology". CRYPTO'92: Lecture Notes in Computer Science No. 740. Springer. (1993), 139-147.

[20]. King S., Nadal S., Ppcoin: Peer-to-Peer crypto-currency with Proof of Stake, 2012, https://archive.org/details/PPCoinPaper.