Blockchain Technology: Applications, Benefits and Challenges

Nursena Baygin
Computer Engineering Department
Kafkas University
Kars, Turkey
nbaygin@kafkas.edu.tr

Mehmet Baygin
Computer Engineering Department
Ardahan University
Ardahan, Turkey
mehmetbaygin@ardahan.edu.tr

Mehmet Karakose
Computer Engineering Department
Firat University
Elazig, Turkey
mkarakose@firat.edu.tr

***Abstract*—Blockchain is the name given to the technology that allows any data set to be stored in a distributed manner. It provides a secure structure with its distributed structure and provides a transparent system with the data set easily accessible by each user. Bitcoin application using blockchain infrastructure has gained attention with its reliability, robustness and performance. Thus, the blockchain is provided to reach large masses. Although the blockchain stands out as the technology of the future, it presents several disadvantages according to the application fields. In this study, blockchains performed on application basis were compared. The advantages and disadvantages of this system, which is called the technology of the future, are examined and compared in detail.**

Keywords—blockchain, security, distributed, consensus

I. INTRODUCTION

The blockchain, called the best invention after the invention of the Internet, attracts attention with its popularity in many areas. It has increased the preferability level with its blockchain reliable structure that presents its difference by offering innovations in many fields such as health, finance, public and industry. Moreover, unlike the classical systems, it has a revolutionary character with the feature that eliminates the central authority [1].

Social media, which has become a part of daily life, provides important data in terms of perceiving user behaviors. Social media provides an unsafe environment with its vulnerable structure at any time and can spread information that will manipulate users. A study in the literature suggested a solution to this unsafe environment. In order to protect the privacy of users, a blockchain based model was proposed and Distributed Partial Ledger Storage Technique (DEPLEST) algorithm was used. With this algorithm, it is ensured that sensitive user information is secured by using less resources than needed in the classical blockchain [2].

As in almost every sector, the blockchain structure in the health sector has been emphasized and various studies have been carried out. In a study conducted, body sensor networks used to monitor patient health information were provided with solutions for security, privacy and efficiency deficiencies. In this study, a hybrid blockchain structure was given priority and transparency and accessibility were taken into consideration and possible attacks were taken [3]. In another study, a blockchain structure was constructed in which patient health information was kept in a distributed manner. In another study, a blockchain structure was constructed in which patient health information was distributed in a distributed manner. Although the system provides the benefits of the classical blockchain, it is seen that the current technology does not meet all the needs of the health system [4].

With the development of the internet, the frequency of use of IoT devices increases day by day. With these increasing devices, the resource requirement increases and at the same time, the inefficient consumption of these resources is faced. In a study conducted to solve this problem, a blockchain based algorithm using secure method to exchange resources (SMER) method was proposed. Devices that do not have similar features are ensured to use secure resources. In this way, IoT devices can share resources among themselves without relying on a central authority [5]. Voting systems are another application area where blockchain structure can be used. With its transparent, decentralized structure and security, it is foreseen that it can be used in voting systems in the future. In a study on this subject, blockchain was created with sequential mining method by using Multichain source codes. In addition, the confidentiality of the voter's identity was ensured by using the blind signing technique. While the established system provides security for voting and counting, it can remain open to attacks in case of online elections [6].

When the studies carried out in the literature are examined, it is seen that blockchain can be used in many fields such as public, health and finance. With its decentralized structure, it can provide reliability, transparency, invariance, accessibility, controllability and data integrity. However, as in every system, there are some deficiencies in the blockchain. Examples of such deficiencies are the need for a very large database, high consumption of electricity, and the creation of conflict problems.

In this paper, the success of the blockchain structure has been investigated and it has been examined what advantages and disadvantages it offers on the basis of sector and application. For this purpose, general information about blockchain is given in the second section of the study and the architecture of this system is explained. In the third section of the study, the application areas of the blockchain are examined and their advantages and disadvantages are presented comparatively. In the fourth and final section, the conclusions are given.

II. BLOCKCHAIN ARCHITECTURE

Blockchain technology is classified according to the characteristics used and whether or not network participation is subject to permission. As can be seen from Figure 1, there are 3 types of blockchain. In open blockchain systems, users do not need permission from any authority. In this type of system, every process can be monitored transparently. Networks such as Etherum, Bitcoin, LiteCoin, Monero are examples of open blockchains. Special blockchains are networks that are wholly authorized by the authority. Who will participate in the network, mining operations, new transactions are subject to permission. With this structure,

978-1-7281-3992-0/19/$31.00 ©2019 IEEE

although it seems to be contrary to the logic of the blockchain, the operations performed are separated from the classical systems with the feature of being seen by each user in a transparent manner. In consortium blockchains, participation in the network is not open to everyone and is based on the approval mechanism. It refers to networks realized between groups coming together for certain purposes. The system is executed in a closed manner and job descriptions are defined. Therefore, there is no need for reconciliation methods. This enables faster execution of transactions [4]. Detailed features of these blockchain types are presented in Table 1, comparatively.

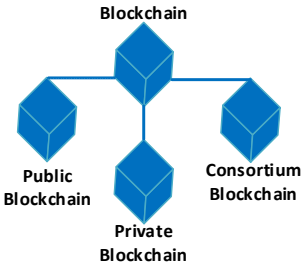

Fig. 1. Blockchain types

TABLE I. THE FEATURES OF BLOCKCHAIN TYPES

Features	Blockchain Types		
	Public Networks	*Private Networks*	*Consortium Networks*
Agreement mechanism	No approval required	Approval required	Approval required
Read permission	Open	Limited	Limited
Productivity	Low	High	High
Centrality	Distributed	Centralized	Distributed-Centralized
Data exchange	Impossible	Changeable	Changeable

A. Hash Functions

The Hash function is a function that takes text as input and converts it to a unique fixed-length array as output. The uni-directionality of hash functions makes these functions irreversible [7]. A block diagram illustrating this situation is presented in Fig. 2.

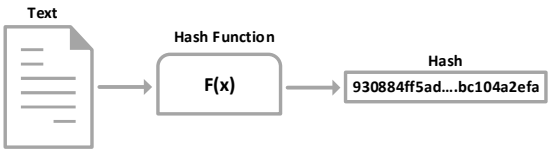

Fig. 2. Hash function

B. Node

The node refers to each device in the network and has two types. One of them, Light node, is used to verify the authenticity of transactions by holding block headers. It is also not obliged to follow the consensus rules. The full node is responsible for keeping all block information and applying the consensus rules [8].

C. Cryptology

Encryption is used to secure the blockchain in case of attack. It is aimed to ensure the confidentiality and integrity of the data. There are two types of encryption for this purpose. These are asymmetric and symmetric encryption types, respectively. In symmetric switching, a single key is used and the same key is used to encrypt and decrypt the data. In asymmetric switching, there are two keys and a mathematical encryption between these keys. With this aspect, asymmetric encryption is more reliable than symmetric encryption [9].

D. Transaction

The transaction refers to the transfer of digital assets between the parties in the blockchain system. The transactions approved by the system are recorded on the blocks and added to the blockchain. An example block diagram of this process is given in Fig. 3 [10].

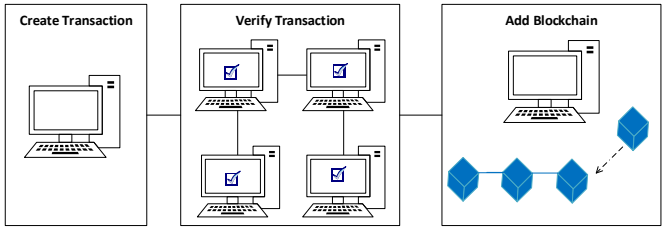

Fig. 3. Transaction steps

E. Merkle Tree

The Merkle tree is a data structure that allows the storage of transactions within the block. There is a summary of the transactions [11]. With the Merkle tree, the download status of the miner's entire database is eliminated, and verification and control is performed only with the help of the block header [12].

F. Consensus Protocol

The consensus protocol is the system that eliminates the central structure used in conventional systems and assigns authority to all nodes in the network. The transparent feature of the blockchain is supported by ensuring that everyone takes responsibility in processes such as approval, supervision and control [13]. Various consensus algorithms have been established. Examples of these are algorithms such as proof of work, proof of stake, proof of authority [14].

G. P2P Network

In central networks, communication between people takes place through a third party. However, the communication between people becomes one-to-one in systems with P2P network structure. This structure, also called distributed network, forms the basis of blockchain logic [15].

H. Ledger

It refers to the book in which all transactions performed in the blockchain are registered. In classical databases, these records are located in a central authority, while in the blockchain, the records are stored by all nodes in the network. In this way, the whole registry is secured and all transactions can be seen in a transparent manner [16].

I. Wallet

Wallet is an application that provides secure storage of keys and digital information of people in the blockchain system [17].

J. Blocks

Block is the area where the transactions on the blockchain network are held. The first block in a blockchain is called a genesis block. A block is basically composed of two parts, the title and the content. The block header is basically composed of the hash value of the previous block, merkle tree, date, degree of difficulty and counter sections. An example image summarizing a block and its contents is presented in Fig. 4.

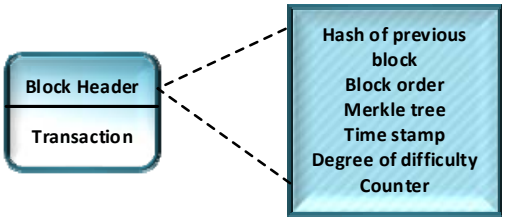

Fig. 4. One block structure

III. Blockchain Application Areas

Initially, the blockchain caused bitcoin to be used only in the field of economy due to the frequent mention of its name. However, contrary to popular belief with the developing technology, the applicability of the blockchain in many areas has emerged. Thus, it has mentioned its name in many sectors with new fields of application day by day. In this paper, the areas where blockchain is used and can be used are examined in detail. In this context, the usage of the blockchain in which sectors and for what purpose has been examined and in addition, possible advantages and disadvantages of blockchain in these sectors were identified. A table summarizing the information obtained within the scope of the study is presented in Table 2. In addition, the blockchain application areas in Turkey are given in Table 3. A graph showing the usage of the blockchain by sectors is given in Fig. 5.

TABLE II. AREAS OF BLOCKCHAIN WITH ADVANTAGES AND DISADVANTAGES

Sector	*Application Area*	*Advantages*	*Disadvantages*	*References*
Governance	• Voting • Land transactions • Tax regulation • Education • Government services • Inheritance • Charities • Labor rights • Authentication	✓ A transparent, reliable, verifiable system ✓ Data security in the event of a natural disaster ✓ Preservation of assets, reporting, availability, cost, effective collateral management	➢ Internet-based systems being vulnerable ➢ System slowing down due to added blocks ➢ Failure to maintain key privacy in all cases ➢ Selfish miners putting the system in trouble	[6], [19], [20], [21], [22], [23]
Health	• Storing medical records • Health Service	✓ Patient data security ✓ System in which the patient is included instead of the system controlled by the central structure ✓ Storage and analysis of health information as a whole	➢ Obligation to train the patient with the inclusion of the patient in the system ➢ Although the blockchain does not allow unauthorized access, it is possible that confidential data will be released due to technical failures	[19], [20], [24], [25]
Finance	• Investment funds • Crypto exchanges • Stock • Insurance • Credit records • Mass funding	✓ Fast, reliable, low cost and simple system ✓ Reliable system thanks to controllable, non-tampering blocks ✓ A recoverable system in case of failure	➢ Difficulty in implementing the entire blockchain structure due to the fact that banking systems implemented in real life need a certain degree of centralization ➢ Increasing the verification time of the system with increasing number of blocks and consequently slowing down the system	[19], [20], [21], [23], [26]
Technology	• Cloud storage • Data backup • Manage the Internet of Things • Messaging applications • cloud computing	✓ Data consistency, rapid verification of operations ✓ Increased productivity, flexibility, low cost by eliminating third-party agents ✓ The formation of fast-moving systems with blockchain open source code shares	➢ Cost and capacity constraints. ➢ Manipulation of data. ➢ Cloud servers are vulnerable to attacks during downtime. ➢ Data theft, take away the system	[5], [19], [20], [23], [27], [28]
Others	• Supply chain • Copyright protection • Food safety • Shared vehicle usage • Internet advertising • Forecasting systems • Energy management • Human rights • Customer recognition systems • Quality control • Logistics • Waste management	✓ Transforming the traditional structure to create reliable, decentralization, scalable and unique structures ✓ Ensuring integrity by creating a common database ✓ Protection of the copyright of the author	➢ 51% of the blockchain is seized and the system is at great risk. ➢ Fork problem in the system. ➢ High cost of converting existing system infrastructure to blockchain structure ➢ Uncertainty about regulations. ➢ Lack of clarity regarding smart contracts. ➢ Synchronization problem on non-interoperable systems	[19], [20], [21], [23], [27], [29]

TABLE III. BLOCKCHAIN APPLICATIONS IN TURKEY

Sector	*Application Area*	*Contribution*	*Mission*	*Title*	*Reference*
Governance	Cadastre Data Management and Update	✓ Preventing data manipulation ✓ Ensuring land management with accurate	A block chain aimed at eliminating inconsistencies in cadastral surveys	Hierarchical Blockchain Architecture for a Relaxed Hegemony on Cadastre Data Management and Update: A Case Study for Turkey	[30]
Finance	Mutual Funds	✓ In this study ıt is predicted that the approval mechanism of pension mutual funds will be fast and reliable	An overview of the blockchain structure is presented. Blockchain has been proposed to be used in the pension fund market in Turkey	Blockchain Technology and Its State in the Financial Services Sector in Turkey	[31]
Technology	Internet of Things	✓ Increased service quality and variety of offers	A block chain has been proposed to collaborate between IoT device vendors and artificial intelligence and machine learning solution providers.	IDMoB: IoT Data Marketplace on Blockchain	[32]
Supply Chain	Agricultural food supply chain proposal	✓ A transparent system used by all users ✓ A system based on mutual trust	Establishing a reliable tool in the system by eliminating the mediator marketplace in Turkey.	Blockchain Design in Agricultural Food Supply Chain: Example of Marketplace Law in Turkey	[33]
Education	Certification verification of open and distance education programs	✓ The proposed system ensured confidentiality, low error and integrity during the certification process	The certificate issued by the state universities in Turkey to provide a solution for verification.	A Blockchain Based Certification System For Education: Bcertificated	[34]

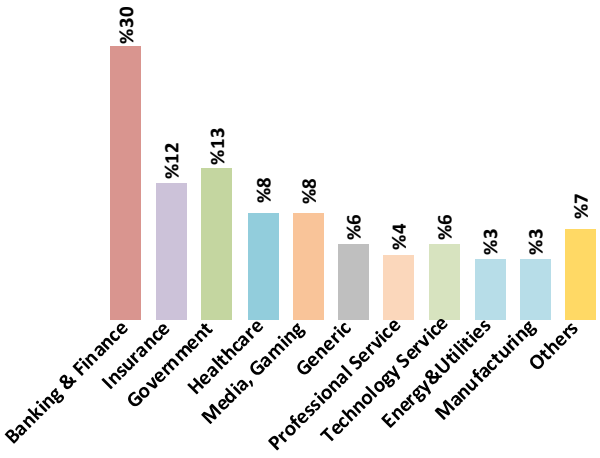

Fig. 5. Use of blockchain by sectors [35]

As can be seen from Fig. 5, especially the financial sector is in the first place in blockchain usage. The second place is the governance sector due to especially, smart contracts. Energy and production sectors are at the end of the list. A graph showing the distribution of the blockchain by continents is given in Fig. 6.

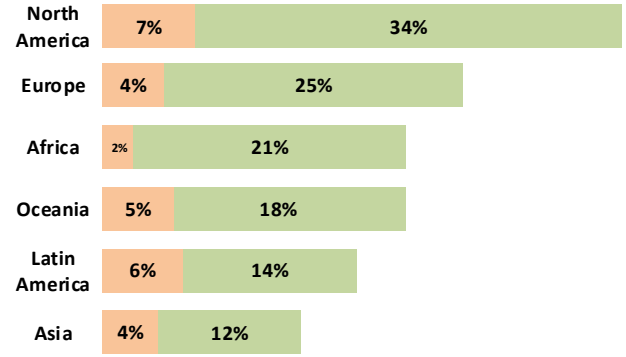

Fig. 6. Use of blockchain according to continents [36]

IV. CONCLUSIONS

Blockchain has attracted attention with its revolutionary features. It has undergone a rapid development process with its applicability, safety and flexibility in almost every sector. Blockchain structure adds basic features such as consistency, speed, scalability and verifiability to the areas where they are applied. However, it is also possible to face difficult problems such as the complete replacement of the infrastructure of traditional systems.

In this study, information about blockchain architecture is given and the situations encountered on application basis are examined. In addition, sector distribution of blockchain usage has been examined and information has been given about the usage of blockchain by continents.

REFERENCES

[1] L.Ismail and H. Materwala, "A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions,"Symmetry, 11(10), vol 1198, 2019.

[2] Y. Chen , H. Xie, K. Lv, S. Wei and C. Hu," DEPLEST: A Blockchain-based Privacy-preserving Distributed Database toward User Behaviors in Social Networks," Information Sciences,2019

[3] I. Jawaid, I.U. Arif, N. Amin and W. Abdul, "Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain," International Journal of Distributed Sensor Networks, 2019

[4] M. Murat, "Blockchain İle Güvenli Elektronik Sağlık Sistemi", İstanbul Technical University, 2018

[5] Z. Yu, H. Yuxing and W. Jiangtao, "SMER: a secure method of exchanging resources in heterogeneous internet of things," Frontiers of Computer Science, 13.6, pp. 1198-1209,2019.

[6] A. E. Muhammed, "Blokzincir Tabanlı Oy Verme Sistemi Öneri," Necmettin Erbakan University, 2018.

[7] E. D. Serap, "Blockchain Teknolojisinin Finans Sektöründeki Yeri ve Uygulamaları, " Marmara University, 2018.

[8] B. Şeref, "A Blockchain –Based Framework for Customer Loyalty Programs," İstanbul Technical University, 2018.

[9] G. Güliz, "Blokzincir Teknolojisiyle Gıda Güvenliği Ve Yumurta Sektörü İçin Örnek Bir Uygulama," Marmara University, 2019.

[10] C. Ç. Salih, "Implementing a Blockchain Protocol and Creating a Digital Asset Transfer Environment",Bahçeşehir University, 2018.

[11] S. K. İmparator, "Elektronik Ödemelerde Blok Zinciri Sistematiği ve Uygulamaları," Erciyes University, 2017.

[12] G. Bilal, "Blok zinciri Tabanlı Elektronik Seçim Sistemi Tasarım Ve Kısmi Uygulaması," İstanbul Technical University, 2019.

[13] Ç. N. Galip, "Blockchain Teknolojisiyle Açık Anahtar Altyapısı Tabanlı Elektronik Sertifika Durum Bilgilerinin Yönetilmesi," Sakarya Uygulamalı Bilimler University, 2019.

[14] A. Kerem, "Blokzinciri Ve Akıllı Sözleşmeler: Güvenli Bir Dijital Sertifikasyon Uygulaması Geliştirilmesi," Trakya University, 2019.

[15] Z.Ü. Evrim, "Blockchain's Impact On Solving Supply Chain Mnagement Challenges," Yeditepe University, 2018.

[16] B.Ç. Doğa, "Blokzincir Tabanlı Elektronik Seçim Sistemi Modellemesi," İstanbul Technical University, 2019.

[17] O. T. Ali, "Blok Zincir Teknolojisi ve %51 Sorunsalı," Beykent University, 2019.

[18] K. İsmail," Blokzinciri teknolojisi ve yakın gelecekteki uygulama alanları," Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 9.1, pp. 75-82, 2018.

[19] S. Hamza,"Gayrimenkul Sektöründe Blok Zincir Teknolojisinin Kullanımı VE Akıllı Kontratların İncelenmesi," İstanbul Technical University, 2019.

[20] Y. Reyhan, "Ürünlerin Tedarikçiden Tüketiciye Ulaşmasını Takip Edecek Bir Blok Zinciri Sisteminin Tasarlanması," İstanbul University, 2019.

[21] A. Mahmut, "Elektronik Para Ve Blockchain'in Finansal Yönetim Üzerine Etkileri," İstanbul T.C. Maltepe University, 2018.

[22] K. Merve,"Blockchain Teknolojisi Ve Akıllı Sözleşmeleriin Yaygınlaşmasının Önündeki Engeller," Bahçeşehir University, 2019.

[23] Z. Zibin, S. Xie, H. Dai, X. Chen and H. Wang," An overview of blockchain technology: Architecture, consensus, and future trends," 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, pp. 557-564, 2017.

[24] M. Matthia, "Blockchain technology in healthcare: The revolution starts here," 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, 2016.

[25] E. A. Mark, "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector," Technology Innovation Management Review, vol 7.10, 2017.

[26] G. Ye and C. Liang, "Blockchain application and outlook in the banking industry," Financial Innovation 2.1, 2016.

[27] L. I. Chang, and T.C. Liao, "A Survey of Blockchain Security Issues and Challenges," IJ Network Security ,vol 19.5 , pp. 653-659, 2017.

[28] K. Nir, "Can blockchain strengthen the internet of things?," IT professional ,vol 19.4 ,pp. 68-72, 2017.

[29] D. Advait, S. Katherine, L. Louise and G. Salil, "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards," Overview report The British Standards Institution (BSI) , pp. 1-34, 2017.

[30] T. Abdulvahit, "Hierarchical blockchain architecture for a relaxed hegemony on cadastre data management and update: A case study for Turkey." Proceedings of the UCTEA International Geographical Information Systems Congress, 2017.

[31] T.Y. Sibel and E.D. Serap, "Blockchain Teknolojisi ve Türkiye Finans Sektöründeki Durumu." Finans Ekonomi ve Sosyal Araştırmalar Dergisi (FESA),vol 4.1, pp. 30-45.

[32] Ö.R. Kazim, D. Mehmet and Y. Arda, "IDMoB: IoT Data Marketplace on Blockchain." 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018.

[33] Y. Abdullah and Ü. Pelin, "Tarımsal Gıda Tedarik Zincirinde Blokzincir Tasarımı: Türkiye'de Hal Yasası Örneği." Bartın Orman Fakültesi Dergisi, vol 21.2, pp. 458-465, 2019

[34] Ö.C. Ayşe, Ö. Şafak, A. Müge and K. Enis, "A Blockchain Based Certification System For Education: Bcertificated." Preface of the Editors(2018), PREFACE OF THE EDITORS (2018), pp. 118-121, 2018.

[35] G. Hileman, M. Rauchs, "Global blockchain benchmarking study", University of Cambridge, 2017.

[36] PwC Global Fintech Report, pp. 1-19, 2017.