Blockchain Technology, Challenges and Current Developments

M. Hanefi CALP
Karadeniz Technical University

Yusuf UZUN
Necmettin Erbakan University

Resul BUTUNER
Beypazari Fatih Vocational and Technical Anatolian High School

Introduction

Knowledge and information is known as the most valuable resource today. Obtained data is transformed into information and information is transformed into knowledge. Thanks to the developing computer technologies, data can be collected in many areas. It is a necessity that the collected data can be easily and securely stored and managed effectively. Due to these needs, database management systems and approaches are developing rapidly (Onder, 2005). In this context, the topics of performance, success, security and query/audit in database systems come to the fore. Currently used database management systems have many advantages and disadvantages. Preventing the access of malicious third parties to data becomes the priority of everyone who stores and manages data, especially public institutions and private sector companies. Malicious third parties are also changing their attack methods day by day with the developing technology and making them more dangerous. All these developments turn today's known safe systems into tomorrow's weakest systems (Vural and Sagiroğlu, 2010).

At this point, the rapidly developing and spreading blockchain technology comes to the fore. This technology is defined as a decentralized distributed database. It is known to be a more consistent and secure database because it is a distributed database. Also finance, education, tourism etc. It is widely used in many different fields such as (Nakamoto, 2008). The innovations and advantages that come with blockchain technology are also important for public institutions and private sector seeking secure databases. Recently, the increasing popularity of blockchain technology and the new approach it has developed have led to an increase in the number of users of this system (Kakavand et al., 2017). Users do not need a third agent when transferring products or services, thanks to the decentralized distributed data structures feature of the blockchain. Thus, a more transparent, reliable and accountable opportunity is provided. As a result of the development of the internet and making communication effective, more and more interactive societies have emerged. As a result, new technologies such as smart phones, smart contracts and the internet of things have been widely used (Tapscott & Tapscott, 2016).

Definition and Features of the Blockchain

Blockchain has different definitions in the literature. According to Nakamoto, a blockchain is a distributed data structure that records every step/transaction information performed by users on the network and shares this information (Nakamoto, 2008). Zheng et al. have been defined the blockchain as a ledger that is stored in blocks as the nodes in the network approve the transactions and grows as new blocks are added (Zheng et al., 2017). According to Beck, the blockchain is a database that allows the transactions to be made consistently and securely by the nodes in the network (Beck, 2018). On the other hand, Glaser defined the blockchain as a ledger shared by all stakeholders, where the records of valuable assets (house, car, contract, etc.) are recorded publicly (without using real identity, if desired) with pseudonyms without the need for a central authority (Glaser, 2017). According to Reyna et al., the blockchain is a distributed, transparent and immutable data structure in which the reliability of every transaction is verified by the nodes in the network (Reyna, 2018). Tama et al. stated that the purpose of the blockchain is not to interfere with the data from the outside, there are blocks approved at every node in the network and it is a part of a distributed software system (Tama et al., 2017).

Technically, blockchain is defined as the integration of distributed ledger, decentralized contract and cryptographic algorithms. Transactions made on blockchain technology are stored in a list of data blocks that are cryptographically linked in a chain. The formation of blocks in the blockchain system is provided by the confirmation of the accuracy and validity of the transactions by the participants in a decentralized network in a distributed structure, and as a result of time-stamped algorithms (Hawlitschek et al., 2018). Zhao et al. revealed that the most important feature of the blockchain system is that it supports transparent and reliable transactions with network-based mathematical calculations instead of human control of transactions. With this feature, the blockchain can be thought of as an "operating system for interactions" (Zhao et al. 2016). Lewis stated that the blockchain is an improved database that provides solutions based on consensus rules for operations such as adding records, verifying and distributing information (Lewis, 2016).

Technical Concepts and Classification of the Blockchain

Basic Concepts

Distributed Ledger Technology (DLT)

DLT is a transparent database where important data or assets of public institutions and private sector companies can be viewed by all users in the network (Pinna & Ruttenberg, 2016). What is meant by distributed ledger is a ledger that can work with its own consensus standards without a central approval system (European Securities and Markets Authority, 2016). Another feature of DLTs is the use of cryptography as a

tool for storing assets and verifying transactions (Wessel, 2016). Transactions performed through DLTs can be cleared and finalized almost instantly, as all information or records will be distributed among all users (Digital Currencies, 2015).

Irreversibility of Records

Every transaction performed in blockchain technology is stored as an endless chain in block lists. Considering the irreversibility of these stored records, some calculation algorithms are used. It is not possible to change the information in a previously created block without breaking the structure of the chain. Therefore, if the data is corrupted, the records are visible to everyone in all the nodes created (Marco & Lakhani, 2017).

End-to-End Communication

Rather than using any centralized structure, individual nodes transmit and store data directly to each other in a peer-to-peer network (Nakamoto, 2008; Marco & Lakhani, 2017; Huumo et al., 2016). Due to the consensus among the nodes in the blockchain system, there is no need for a specific center and intermediaries (Pilkington, 2016). In the blockchain, information is stored by all participants (nodes) in the BitShares chain (Marco & Lakhani, 2017). Some authors argue that transactions created in the blockchain are not recorded by all nodes, but can be used (Nakamoto, 2008; Huumo et al., 2016).

Transparency

The concept of transparency in blockchain occurs when the participants in the network can see all transactions and blocks (Marco & Lakhani, 2017; Huumo et al., 2016). This suggests that the blockchain system is more transparent than a centralized system managed by a third party. Most of the sources state that the blockchain technology is open source, that is, it does not have a specific owner (Huumo et al., 2016; Tian, 2016).

Computational Logic

Since the BitShares chain is located in a digital environment, the computational logic can be realized according to the transactions in the blockchain. Nodes can use rules and algorithms to trigger transactions/processes automatically. BitShares transactions can be programmed to handle any type of information (Marco & Lakhani, 2017).

Classification of Blockchain Systems

Blockchain systems are classified under three headings (Buterin, 2015; Puthal et al., 2018; Zheng et al., 2017).

Public Blockchain

It provides an open permissionless platform that enables individuals affiliated or independent of various institutions or organizations to participate and mine. In this type of blockchain, there are no barriers or restrictions on entry to the blockchain. That's why the Public blockchain is also known as the permissionless blockchain. Public Blockchains are completely open and transparent and do not contain any private validator node, that is, a node that controls the transactions or that requires permission to enter the block.

They are blockchain structures that allow data exchange between individuals in the organization and are managed by a participant or group of participants in the network. Such blockchains are also known as permissioned blockchains. Because participants who do not have a special permission cannot join the chain. A node's access to and participation in the network is done by the group that manages the network according to the set rules. This situation reduces the level of compliance with the decentralized and transparent nature of blockchain technology.

Consortium Blockchain

It is defined as a private and permissioned blockchain technology in which a previously identified group of nodes is the authority/decision maker instead of a single transaction in the block verification and consensus process. These nodes identify the participants who can join the network and mine. Block validation is only valid if a block is signed by authorized nodes. A consortium decides that the network is public and that anyone on the network can read/write data. A comparison of all blockchains is given in Table 1.

Table 1. Comparison of the Blockchains

	Public Blockchain	Private Blockchain	Consortium Blockchain
Settlement Providers	All Miners	An Organization	Selected Nodes
Read Permissions	Open	Open or Allowed	Open or Allowed
Efficiency	Low	High	High
Centralization	No	Yes	Partially
Participation in Settlement Procedures	Without Permission	Permitted	Permitted

Challenges and Current Developments

Although blockchain technology has very important advantages and possibilities, it also has some limitations and difficulties. In this section, both these (difficulties) and possible solutions are given.

Scalability

With the number of transactions increasing day by day, the volume of blockchain systems is also increasing. Each node in the blockchain system must store all blockchain data. The purpose here is to perform verification and reconciliation transactions. However, this situation causes the blockchain structure to grow much more (Zheng et al., 2017). Due to some difficulties such as the capacity of the blocks and the speed of publishing, the number of confirmed transactions in the chain in a certain period of time is limited (Vukolić, 2015). The fact that miners prioritize large transfers and ignore small transactions causes delays in transaction time (VISA Fact Sheet, 2021).

Privacy

Users can transact with their own public and private keys without using their real identities. At the same time, data such as sender, receiver, time and transferred value are publicly published because transparency is essential (Meiklejohn, et al. 2013). Two concepts, namely anonymization and mixing, have been developed against privacy violations that may be encountered in the blockchain.

Anonymization

A zero-knowledge proof method is used, which allows verification with a one-sided password in order to hide (ensure privacy) of user information. This process is done instead of verification with digital signature and mining. Thus, the activities or relationships between the person and the transfer process remain confidential (Sasson et al., 2014).

Mixing

The scrambling service enables data to be collected from multiple sending addresses and forwarded to multiple receiving addresses. Recipient addresses are mixed by a central scrambling server to prevent theft. Thus, both encryption and address mixing methods are used (Bonneau et al., 2014; Van Wirdum, 2016; Ruffing et al. 2014).

Blocking Attack (Selfish Mining)

Malicious miners put the blocks they create on hold before releasing them and issue their private chain branches. They do this by using their own blocks after the necessary conditions are met. As a result, a bifurcation occurs in the chain. Malicious miners cause competitors to waste their power and time and can gain unfair advantage (Heilman, 2014).

Conclusion and Recommendations

In this chapter, blockchain technology, current developments and challenges are presented. Blockchain technology is a current technology and has a great development and transformation potential in many areas. First of all, when evaluated in terms of advantages and disadvantages of blockchain technology, it has been seen that it will replace traditional database systems. In addition, with these systems, very successful results can be obtained in terms of data security, consistency and data transfer. The privacy, transparency and distributed nature of blockchain technology provides advantages against central authorities. However, features of blockchain technology such as verification, system performance and querying can sometimes be a disadvantage. In addition, when we look at this technology from the perspective of the financial sector, it can be said that performance is a big handicap. In existing systems, thousands of transactions are performed instantaneously per second. It has been observed that these numbers are very low in the blockchain. The verification of transactions in the blockchain enables transactions to be made with big data. This has an impact on performance and productivity.

Along with blockchain technology, many innovations have entered our lives. In addition, it can be said that there is a great need for data analysis of the blockchain system. With the developments in blockchain technology, artificial intelligence creates new opportunities and approaches in applications. These technologies have superiority over traditional systems thanks to their secure and efficient data transfer features. As a result, projects and investments related to blockchain technologies should be made and this technology should be supported to develop and spread faster.

References

Beck, R. (2018). Beyond bitcoin: The rise of blockchain world. *Computer*, *51*(2), 54-58.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., & Felten, E. W. (2014, March). Mixcoin: Anonymity for bitcoin with accountable mixes. In *International Conference on Financial Cryptography and Data Security* (pp. 486-504). Springer, Berlin, Heidelberg.

Buterin, V. (2015). On public and private blockchains. *Ethereum blog*, *7*(1). https://blog.ethereum.org/ 2015/08/07/on-public-and-private-blockchains/.

Digital Currencies, Committee on Payments and Market Infrastructures, Bank for International Settlements (November 2015), available at http://www.bis.org/cpmi/publ/d137.pdf.

European Securities and Markets Authority, Discussion Paper, The Distributed Ledger

Technology Applied to Securities Markets, p. 8 (June 2, 2016) available at https://www.esma.europa.eu/sites/default/files/library/2016- 773_dp_dlt.pdf

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic commerce research and applications*, *29*, 50-63.

Heilman, E. (2014, March). One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. In *International Conference on Financial Cryptography and Data Security* (pp. 161-162). Springer, Berlin, Heidelberg.

Kakavand, H., Kost De Sevres, N., & Chilton, B. (2017). The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. *Available at SSRN 2849251*.

Lewis, A. (2016). So, You Want to Use a Blockchain for That?. *Coin Desk*, *22*. https://www.coindesk. com/want-use-blockchain/

Marco, I., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118-127

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference* (pp. 127-140).

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260. https://bitcoin.org/bitcoin.pdf.

Onder, E. (2005). Yönetim Bilişim Sistemleri Kapsamında Web Tabanlı İlişkisel Veritabanı Yönetim Sistemleri ve Bir Uygulama. *İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Sayısal Yöntemler Bilim Dalı, Yüksek Lisans Tezi, İstanbul*.

Pilkington, M. (2016). "Blockchain technology: principles and applications". Research handbook on digital transformations, 225.

Pinna, A., & Ruttenberg, W. (2016). Distributed ledger technologies in securities post-

trading revolution or evolution?. *ECB Occasional Paper*, (172). https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine, 7*(4), 6-14.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems, 88*, 173-190.

Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2014, September). Coinshuffle: Practical decentralized coin mixing for bitcoin. In *European Symposium on Research in Computer Security* (pp. 345-364). Springer, Cham.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy* (pp. 459-474). IEEE.

Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K. H. (2017, August). A critical review of blockchain and its current applications. In *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)* (pp. 109-113). IEEE.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.

Tian, F. (2016, June). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In *2016 13th international conference on service systems and service management (ICSSSM)* (pp. 1-6). IEEE.

Van Wirdum, A. (2016). Coinjoin: Combining bitcoin transactions to obfuscate trails and increase privacy. *Bitcoin Magazine.[Online]. Available: https://bitcoinmagazine.com/articles/coinjoincombining-bitcoin-transactions-to-obfuscate-trails-and-increase-privacy-1465235087/.[Accessed: 14-Oct-2021]*.

VISA Fact Sheet, https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf, 10.11.2021.

Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International workshop on open problems in network security* (pp. 112-125). Springer, Cham.

Vural, Y., & Sağıroğlu, Ş. (2010). Veritabanı yönetim sistemleri güvenliği: tehditler ve korunma yöntemleri. *Politeknik Dergisi, 13*(2), 71-81.

Wessel, D. (2016). Hutchins Center Explains: How Blockchain could change the financial system. *Brookings, January, 11*. Quarterly Bulletin, 2014:Q3).

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?, A systematic review. *PloS one, 11*(10), e0163477.

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE.

About the Authors

M. Hanefi CALP received Ph.D. degree in 2018 from the department of Management Information Systems at Gazi University, one of the most prestigious universities in Turkey. He works as Associate Professor in the department of Management Information Systems of the Faculty of Economics & Administrative Sciences of the Karadeniz Technical University. His research interest includes Management Information Systems, Artifical Neural Networks, Expert Systems, Fuzzy Logic, Risk Management, Risk Analysis, Human-Computer Interaction, Technology Management and Project Management.

E-mail: mhcalp@ktu.edu.tr, ORCID: 0000-0001-7991-438X.

Yusuf UZUN, PhD, is an Assistant Professor of Computer Engineering at Necmettin Erbakan University in Konya, Turkey. He holds a PhD in Mechanical Engineering from Necmettin Erbakan University. His main areas of interest are artificial intelligence, autonomous systems and augmented reality applications. He also works as the Rector's Advisor at Selcuk University.

E-mail: yuzun@erbakan.edu.tr, ORCID: 0000-0002-7061-8784.

Resul BUTUNER is a Computer Teacher at Adil Karaagac Vocational and Technical Anatolian High School in Konya, Turkey. He has a master's degree in Computer Engineering from Necmettin Erbakan University. His main areas of interest are artificial intelligence, robotic coding, data mining and augmented reality applications. He is an instructor in the field of Robotic coding within TUBITAK. He continues to write a book in the field of robotic coding at the Ministry of National Education. He worked as a coordinator in budgeted projects related to student education.

E-mail: rbutuner@gmail.com, ORCID: 0000-0002-9778-2349.

To Cite This Chapter

Calp, M.H., Uzun, Y., & Butuner, R. (2021). Blockchain technology, challenges and current developments. In M. Ozaslan & Y. Junejo (Eds.), *Current Studies in Basic Sciences, Engineering and Technology 2021*(pp. 60–69). ISRES Publishing

Copyright © 2021 by ISRES Publishing