DISCUSSION PAPER

Blockchain Technology:
Miracle or Mirage?

Murat Selvi

TRT WORLD
research centre

DISCUSSION PAPER

Blockchain Technology:
Miracle or Mirage?

Murat Selvi

TRT WORLD
research centre

© TRT WORLD RESEARCH CENTRE

ALL RIGHTS RESERVED

WRITTEN BY

Murat Selvi

PUBLISHER

TRT WORLD RESEARCH CENTRE

March 2023

TRT WORLD İSTANBUL

AHMET ADNAN SAYGUN STREET NO:83 34347

ULUS, BEŞİKTAŞ

İSTANBUL / TURKEY

TRT WORLD LONDON

PORTLAND HOUSE

4 GREAT PORTLAND STREET NO:4

LONDON / UNITED KINGDOM

TRT WORLD WASHINGTON D.C.

1819 L STREET NW SUITE 700 20036

WASHINGTON DC

www.trtworld.com

researchcentre.trtworld.com

The opinions expressed in this discussion paper represent the views of the author(s) and do not necessarily reflect the views of the TRT World Research Centre.

Introduction

Blockchain technology, which gained recognition with the emergence of Bitcoin, a virtual currency, in 2008 and has remained on the agenda since then, is an important invention that might completely transform the digital universe and all related sectors. On the other hand, it is logical in theory but not very functional in practice. It can be described as a kind of registration system.

The first common misconception about this technology is that it originated in 2008 and was developed by Satoshi Nakamoto. However, the technology in question started to be addressed before the internet, and the theoretical foundations of the subsystems necessary for its implementation became widespread. Blockchain, first mentioned in 1976, refers to recording each transaction on a decentralised network structure built on the logic of peer-to-peer sharing. Instead of any central authority or a single repository, it is a shared ledger of information bundles updated and linked across all participants.

Based on the idea that data is available to all users simultaneously instead of being stored in single or several centres, blockchain offers advantages such as preserving data more securely and making it difficult to change. At this point, again, a common misconception is that it is impossible to change the data. However, in the words of Satoshi Nakamoto, who led this technology to be well-known to large masses through Bitcoin, changing data depends on CPU power and the fact that more than half of the users are well-intentioned. So, yes, the fact that the users in the system are honest people is directly proportional to the reliability of the data.

This technology, a chain created by articulating information blocks containing the data in the previous block, called blockchain, offers many possible advantages due to its underlying logic and potential. However, like all existing technological tools, no technology is independent of the preferences and qualitative characteristics of the people who will use that technology, regardless of its structural features and potential.

Although blockchain is often considered a financial tool, especially since transactions can be tracked openly and transparently, it can be used in many sectors, such as production, transportation, trade, law, media, land registry, real estate, and public services. With the increase of digitalisation, although transactions in many sectors have already accelerated and become much easier to handle, the need for a third intermediary to ensure mutual trust in many issues still needs to be addressed. The most important promise of blockchain technology is that a peer-to-peer transaction can be established by eliminating the need for this intermediary.

It is not a third authority that will provide confidence in each peer-to-peer transaction, but each step and the accuracy of the transactions can be observed and approved by all users included in the system. In other words, as soon as everyone knows everything about the transaction and confirms its accuracy, mutual trust will be established, and the transaction will take place. This paper discusses blockchain technology and ensuing questions about sustainability, trust, inclusivity, and access.

The New Story of Old Technology

Every technological innovation might emerge with some exaggerated rhetoric in its initial period of popularity. They also might have some potential that makes these exaggerations justified to a certain extent. However, it should be remembered that the potential and operation of any tool can only be functional in line with the preferences of the human resource using that tool. Moreover, the benefit or harm it will provide is not independent of the purposes of the person, institution or company that produces or holds the relevant technology. For example, television has been described as a great educational tool, the internet as a decentralised communication network, and social media platforms as new opportunities for a democratic public sphere. At this point, we can observe that all these technological innovations cannot fulfil these exaggerated tasks attributed to them and even produce many results contrary to the initial overly positive expectations.

Blockchain is now known to many people thanks to cryptocurrencies, but there are many questions that need to be answered. Blockchain's most basic premise is to be a globally distributed public ledger. It is indisputable how vital knowledge and recording knowledge have been throughout human history. The ability to keep records has been one of the primary needs of every period and community, dating back to the invention of writing and numbers (Clayton, 2019). Although the skill of keeping records touches every aspect of daily life, it has emerged as a need primarily to carry out trade and production in better conditions, and people have resorted to writing and calculus based on this need (Brown, 2021). According to archaeological research, record-keeping activities were carried out by the Sumerians and Ancient Egyptians, who wrote by etching symbols on tablets (Clayton, 2019). The development of recording information enabled trade and production to be carried out more safely and efficiently. Even the emergence of money was made possible by the ability to keep records. Money is a recording tool that indicates the presence of a precious metal. The Lydians first used money, and the historical journey of money continued until today's digital currency (Jacobs & Slaus, 2012).

This overview reveals how vital recording has been throughout history. Written sources and findings from archaeological research shape our knowledge of all known human history. In addition, the emergence of commercial relations across societies, their economic structures, and the emergence of banks and banknotes have been possible with the acquisition of record-keeping skills. Banknotes, circulated through bankers, are essentially a bill showing that the banker has an appropriate number of valuable metals or provisions. So, it is a registration document. The states monopolised the privilege of printing money. The seemingly ordinary piece of paper (banknote) is essential to shopping and trade.

State authority attributes value to these papers with certain symbols and numbers, allowing a simple piece of paper to express an assigned amount of value and be circulated as money. Therefore, people can offer money, which is more easily transportable, instead of exchanging products. In this transaction, people rely on a central authority, namely the government, central bank, or other banks, for money's value. People trust money, especially the US dollar, the British pound, and other powerful currencies. This trust is due to the reputation of the authority that assigns the value to the currency rather than the piece of paper itself. In short, the money we use is nothing more than pieces of paper with nominal value. Consequently, all registration procedures, such as agreements, contracts, and inheritance, can become effective with a trusted authority's approval, seal, or acceptance.

The US dollar, which started to be used as a reserve currency worldwide after the Second World War, is an important point in the historical journey of money (Best, 2022). The central banks of other governments started collecting the money printed by the US, and almost all nations used the US dollar in trade. Moreover, after a while, the American state suspended the then-normal practice of printing money only proportional to the amount of gold it had, and instead started printing unlimited money, attributing the desired financial value to a simple piece of paper without being indexed to any precious metal. With the help of its current military and economic power and its authority in the world, it has been accepted by nearly all other countries in some way, and the dollar has become the US' most significant power for a long time.

It is essential to be aware of the need for a registry system, the emergence of money, and its journey through history to understand the reasons for the importance attributed to blockchain technology. Trade and transactions have been essential for all societies throughout history and have become the most critical elements underlying all developments, wars, and conflicts.

What Exactly does Blockchain Promise?

At this point, the most fundamental change brought forward by blockchain technology is that it can eliminate the need for the presence of a third party or an authority. Due to the level reached by digitalisation, we can already use money digitally; we can now shop without the need for magnetic cards, signed contracts, and recorded information in completely digital environments. From this point of view, the basic premise of blockchain technology is not the digitisation of money. Due to the publication of the famous 2008 article, cryptocurrency and blockchain were frequently mentioned together, which also led to many misunderstandings (Nakamoto, 2008). As the first type of cryptocurrency, Bitcoin works using blockchain technology, but this application is only one of many transactions that can be conducted using blockchain technology.

The structure, which functions as a peer-to-peer, decentralised registry, works by keeping the entire transaction history on all devices included in the system. A few months after the article was published under the pseudonym Satoshi Nakamoto, the first crypto money bitcoin system was commissioned in 2009, and transactions were opened publicly to all participants. However, as of 2010, the person or group using the pseudonym Satoshi Nakamoto has disappeared, and his/their identity is still unknown.

The Bitcoin system is a database simultaneously logged and distributed across thousands of devices. In the Bitcoin system, defined in the aforementioned article as peer-to-peer digital money transfer, all transactions are carried out simultaneously on all devices connected to the network so that all participants can control the transaction steps. In other words, when a transaction is requested, all transactions from the first block to the last block are accessible to all participants. Beyond storing data on multiple servers, bitcoin promises decentralisation and security because of the simultaneous availability of data on all devices included in the system (Catalini & Gans, 2019).

As it is known today, many companies, banks, institutions, and platforms keep their data on more than one server in many different regions instead of a single server. Among the primary purposes of this application is to provide faster access to the data locally and to ensure that there are many backups of the data in case of any cyber-attack. However, no matter how many copies there are, all data is controlled by the relevant company, firm or institution and is supervised by a central authority. The motivation behind Bitcoin and its derivatives and even the earliest studies of blockchain technology are a revolt against the control and supervision of this paramount authority.

(Meiramgul Kussainova - Anadolu Agency)

Simply put, a chain formed by articulating blocks of information with specific robust encryption methods is managed simultaneously by everyone involved in the system. In theory, all users can confirm the correctness or inaccuracy of the transaction (Nakamoto, 2008). However, data can only be entered into the system, or the chain, while previously recorded data or blocks cannot be easily deleted or changed. Each new transaction, that is, the block, carries the signature of the data in the previous block. In other words, each block in the chain also contains the data recorded in the last block. Therefore, a single transaction change or deletion in any block cannot be done easily. The transaction made on any of the blocks will necessitate changing all the blocks that follow. This working logic substantiates the statements lauding blockchain technology for its security, as the process makes data change nearly impossible. However, it is a common misconception to consider that the system can never be changed or broken.

As with all existing digital systems, systems working with blockchain infrastructure contain security vulnerabilities and cannot provide 100% protection against threats. This is also stated in the article in which Bitcoin was introduced (Nakamoto, 2008). However, if most users are honest, blockchain can work reliably. In other words, if most of the processing power required to carry out transactions is in the hands of honest and reliable people, reliability can be ensured; otherwise, malicious people can manipulate the entire chain as they wish.

After understanding the working principle, the first question that comes to mind is how it will be possible for all participants or users to manually approve or reject any transaction at any time. Apart from having a huge storage area to record the data of all trades, it requires deep technical knowledge to compare the data contained in the blocks for each new transaction at the beginning of the device and to confirm or deny its correctness or inaccuracy. At this point, devices called nodes, which contain a copy of the entire chain and automatically control approval-rejection transactions, come into play (Nigeria, 2021). These devices, thought to be thousands worldwide, serve as a kind of server, but they are organised based on a distributed network model, each connected to the other. In this way, many users in the system can benefit from the possibilities offered by a system that automatically processes within the framework of specific rules and algorithms in the background instead of having a copy of the entire chain on their device or manually approving or rejecting each transaction.

The most cited potential benefit for blockchain technology and bitcoin is that it eliminates the need for money to exist as a powerful tool under the control of a central authority. In other words, blockchain technology could spell the end of fiat money and the beginning of the use of cryptocurrencies based on blockchain tech. Thus, the production, use, and control of money are transferred from the banks and, more broadly, from the state to everyone involved in the system. If such a system becomes widespread and used by all, a global currency that official institutions cannot follow, interfere with, or seize, and has no borders will have entered circulation. According to the idea owners, the peer-to-peer distributed network will act as a means of security, decentralisation and freedom while making all transaction steps open to everyone's scrutiny while providing users with a significant opportunity to remain anonymous (Monrat, Schelen, & Andersson, 2019).

These propositions, presented as beneficial to society and individuals, contain many question marks. As seen in the case of social media, the latter was expected to function as tools that would contribute to social participation and the advancement of democratic principles but were turned into environments that fuel disinformation and polarisation. Similarly, crypto money platforms working with blockchain infrastructure can cause many problems. With its rapid spread in many countries, it is used in many cases of fraud, money laundering, financing of crime and terrorist organisations, and drug and smuggling activities (Leaders, 2015). In addition, due to its structural features, it is possible to control and limit each coin desired to be spent. In other words, expenditure can only be made if the system allows it. Who will operate the system according to the rules determined and who can have the highest processing power are separate discussion topics. For example, Bitcoin is configured to generate 21 million coins, and the reason for this limitation has yet to be apparent.

Moreover, more than half of the bitcoins ever produced are in the hands of a small group of unknown actors. The reason for limiting Bitcoin production (21 million) and making it more challenging (every four years) is expressed as an effort to prevent value decline. This is an essential similarity that causes it to be compared to gold. Gold is one of the limited and, therefore, precious elements found in nature. Its value varies for several reasons, but it is still a valuable mineral worldwide. With a similar logic, possibly, Bitcoin was programmed to be limited, and even the date on which the last bitcoin will be produced (2140) has been declared. Bitcoin operates within the framework of some technical rules. For example, the production of each block can be carried out in 10 minutes, and the difficulty level increases gradually while the reward earned from each new production decreases (Nakamoto, 2008). Therefore,

the date on which the last bitcoin will be generated can be clearly stated because of these rules. In addition, statements have been put forward that limiting the total bitcoin amount can protect people from inflation resulting from decreased value due to the abundance of money. However, it is unclear how this proposition, which seems quite functional in theory, can deliver this expected contribution while a considerable amount of all bitcoins is in the hands of a minority. In addition, it is unclear why Satoshi Nakamoto set up the rules this way.

Moreover, today, Bitcoin and its derivatives, which should function as a decentralised currency, have been generally evaluated over an existing fiat currency, the dollar. The crypto cash that occurred to make direct transfers between peers has turned into securities bought and sold in exchange for dollars. People buy and sell cryptocurrencies using the fiat money they have through their accounts in the crypto money market, and they assume that they are investing as if they have bought a stock, land, or house. The most important reason for this situation might be that the value of Bitcoin, the first cryptocurrency, has reached astronomical figures over the years. This has been very tempting for many, but the process has caused a severe financial loss for thousands of people. Crypto exchanges still need a legal basis and lack all the usual precautions and security measures for the stock market. But some assumptions such as security, immutability, indestructibility, and decentralisation, often attributed to blockchain technology with an exaggerated discourse, can lead to devastating results combined with the ambition of quickly making high profits.

As mentioned above, the production of digital money is not the only use of blockchain technology. Blockchain technology also offers advantages that may lead to sectoral changes in many areas, such as health, property, transportation, manufacturing, and law (Polaris, 2022). Today, some companies providing international transportation services can save time and cost through blockchain-based smart contract applications instead of transactions such as legal procedures and contracts that cause time loss for transportation services. As it is known, digital signatures have been used for a while, and people can sign documents digitally. But with a fundamental difference, blockchain takes the digital verification process to another level. While the digital signature process is costly and time-consuming, requiring the identification and approval of a central authority, the need for a third party is eliminated in smart contracts using blockchain. In this way, an automatic process operates, where permits are carried out as the conditions are met at a much lower cost and in a much shorter time.

Transactions recorded in the digital environment and open to instant control by all parties provide significant advantages for companies. In addition, non-fungible tokens (NFTs), an essential item on the agenda recently, are digital assets that are possible thanks to blockchain technology. NFTs also have the potential to generate economic value, with many examples of this available (Kshetri, 2022). Furthermore, the records of the transactions can be the most reliable ones. When records are open to the public, and all participants can view who owns any digital material, there is no need for any other authority to keep official documentation, such as copyrights or patents.

NFTs are expressed as non-fungible (non-exchangeable) tokens. This characterisation means that, unlike Bitcoin and other similar crypto coins, these tokens are not interchangeable; they cannot be exchanged or reproduced. However, they can be sold or bought at the desired price (Kshetri, 2022). NFTs are datasets that prove ownership and authenticity of any digital asset on a distributed network. A radical change can occur in the digital universe when all art and media content start leveraging blockchain technology to eliminate copyright infringement. In the economy of the ever-growing digital universe, NFTs can generate income for media content producers, artists, and other NFT owners. There is a widespread belief that an NFT is never changeable, but it is as secure as any blockchain token. In other words, the processing power necessary and the requirement that most users be honest are valid in all blockchain-based technological innovations.

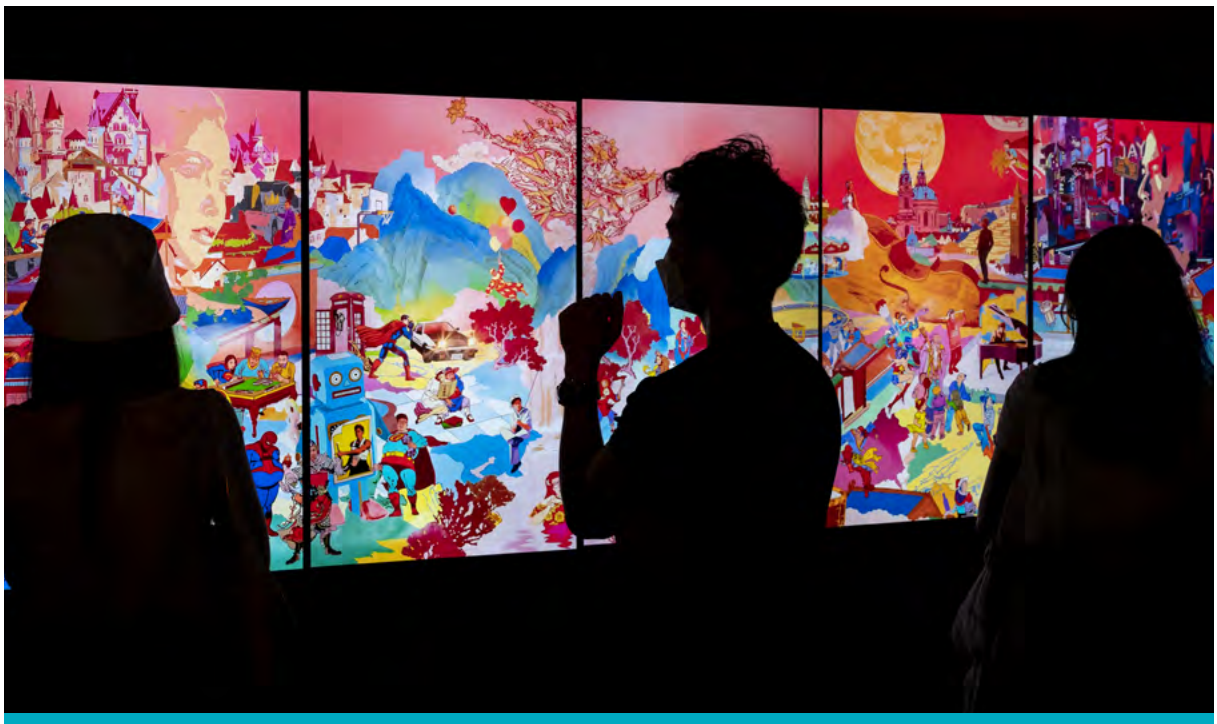
In many countries, studies are carried out to save essential state records on platforms based on the blockchain more securely and at a much lower cost. Moreover, many central banks have started working to produce digital currencies or cryptocurrencies (Bagis, 2022).

Conclusion

Blockchain technology, which combines many different technological applications since the 1970s, is a peer-to-peer distributed network. Hash coding (Back, 2002), timestamping data (Haber & Stornetta, 1991), untraceable digital money (Chaum, 1982), double transaction prevention formula, secure encryption, and electronic cash (Nakamoto, 2008) can be considered as the keystones for the development of the technology. However, despite providing solutions for some problems encountered in the digital universe since the start of the age of the internet, it is also possible that blockchain technology may cause new problems in terms of sustainability, energy consumption, lack of standardisation and security (Monrat, Schelen, & Andersson, 2019).

The lack of detailed information about blockchain technology and its complex mathematical operations and technical information has caused many to prefer avoiding the new phenomena. However, for the same reasons, others have seen it as an investment tool that can assist in making a profit in a short time. This assumption has also led people in many countries to experience severe financial loss while participating in its use. After bitcoin, numerous cryptocurrency types, described as altcoins, have been released. People have invested considerable sums in these digital assets as if they were investing in companies on the stock market. Moreover, most people bought the coins on the websites of the service providers, not by being included in the distributed network, which led them to lose all their savings as soon as the relevant platform was shut down (Wood, 2022).

Bitcoin was introduced in the same year as the global economic depression that started in 2008. That may have contributed significantly to the rise of Bitcoin while the confidence in the currencies controlled by the central authorities decreased. Cryptocurrencies, NFTs, smart contracts, and all other usage areas possible with the blockchain infrastructure will remain on the agenda for a while. But, like almost every technological innovation, blockchain technology, despite all its possible advantages and potential, can only be fully evaluated when it is widely used because no technology is independent of the purpose and qualitative characteristics of the audiences that use it. Blockchain is still in its early stages and continues to evolve. Nevertheless, thanks to Bitcoin, it has become perceived more as a digital investment instrument than the peer-to-peer transaction system it originally was.



(Miguel Candela - Anadolu Agency)

Bibliography

Back, A. (2002, August 1). Hashcash - A Denial of Service Counter-Measure. Retrieved from Hashcash: http://www.hashcash.org/papers/hashcash.pdf

Bagis, B. (2022). Digital Currencies and Monetary Policy in the New Era. Insight Turkey, 189-211. Retrieved from https://www.insightturkey.com/article/digital-currencies-and-monetary-policy-in-the-new-era

Best, R. (2022, September 24). How the U.S. Dollar Became the World's Reserve Currency. Retrieved from Investopedia: https://www.investopedia.com/articles/forex-currencies/092316/how-us-dollar-became-worlds-reserve-currency.asp

Brown, S. (2021, April 27). Where Did Writing Come From? Retrieved from Getty: https://www.getty.edu/news/where-did-writing-come-from/

Catalini, C., & Gans, J. S. (2019). Some Simple Economics of the Blockchain. Rotman School of Management Working Paper No. 2874598 MIT Sloan Research Paper No. 5191-16.

Chaum, D. (1982). Blind Signatures for Untraceable Payments. Retrieved from Sceweb: https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF

Clayton, E. (2019). A history of writing. Retrieved from British Library: https://www.bl.uk/history-of-writing/articles/where-did-writing-begin

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. Journal of Cryptology, 99-111.

Jacobs, G., & Slaus, I. (2012, October 24). https://www.cadmusjournal.org/article/issue-5/power-money. Retrieved from Cadmus: https://www.cadmusjournal.org/article/issue-5/power-money

Kshetri, N. (2022). The Rise of Blockchains. Edward Elgar Publishing.

Leaders. (2015, October 31). The trust machine: How the technology behind bitcoin could change the world. Retrieved from The Economist: https://www.economist.com/leaders/2015/10/31/the-trust-machine

Monrat, A. A., Schelen, O., & Andersson, K. (2019). A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities. IEEE Access, 117134-117151.

Nakamoto, S. (2008, October 31). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from Bitcoin: https://bitcoin.org/bitcoin.pdf

Nigeria, G. (2021, November 22). Types of nodes in the Bitcoin network. Retrieved from The Guardian: https://guardian.ng/technology/types-of-nodes-in-the-bitcoin-network/

Polaris. (2022, June). Blockchain Technology Market. Retrieved from Polaris Market Research: https://www.polarismarketresearch.com/industry-analysis/blockchain-technology-market

Wood, Z. (2022, August 29). Crypto crash: how a teacher's dream investment turned into a nightmare loss. Retrieved from The Guardian: https://www.theguardian.com/technology/2022/aug/29/crypto-crash-how-a-teachers-dream-investment-turned-into-a-nightmare-loss

TRT WORLD
research centre

TRTWORLD
research
centre