

Marcin Brol

Wroclaw University of Economics and Business

e-mail: marcin.brol@ue.wroc.pl

ORCID: 0000-0003-2203-4036

THE INFLUENCE OF BLOCKCHAIN TECHNOLOGY ON EXCHANGE SAFETY AND COSTS

WPLYW TECHNOLOGII BLOCKCHAIN NA BEZPIECZEŃSTWO I KOSZTY WYMIANY

DOI: 10.15611/pn.2020.3.02

JEL Classification: D86

Summary: The goal of this paper is to show the impact of blockchain technology on transaction costs, as well as to show the factors which increase exchange safety when using the blockchain and to point out the potential problems with this technology. A blockchain is an open source, decentralized database, using the Internet and peer-to-peer architecture to register transactions. The potential of this technology leads to the hypothesis that it may become the equivalent of the invisible hand of traditional market exchange, meaning primarily the autonomy of transactions that use it. Blockchain is a mechanism which allows to enforce the execution of agreed contracts through encryption. The qualities of blockchain technology bring the transactions made with its use closer to the conditions of a perfectly competitive market, especially when it comes to transparency and supply and demand dispersion. This results in the diminished ability to influence the price on both sides of the market.

Keywords: blockchain, network economy, peer-to-peer, market exchange, transaction costs.

Streszczenie: Technologia blockchain znana jest przede wszystkim z zastosowań związanych z funkcjonowaniem kryptowalut. Tymczasem spektrum związanych z nią możliwości jest o wiele szersze. Ze względu na to, że funkcjonuje ona w oparciu o protokół peer-to-peer, z powodzeniem może być i jest wykorzystywana wszędzie tam, gdzie przedmiotem obrotu są dobra cyfrowe lub do transakcji dochodzi z użyciem danych w postaci cyfrowej, a więc w przypadku wszystkich transakcji księgowanych lub rejestrowanych w systemach komputerowych. Potencjał tej technologii pozwala na sformułowanie hipotezy, że w gospodarce sieciowej stanie się ona odpowiednikiem niewidzialnej ręki, utożsamianej z wymianą rynkową. Chodzi tu przede wszystkim o autonomiczność dokonywanych za jej pomocą transakcji. Dzięki zastosowaniu technologii blockchain rynek w gospodarce sieciowej stanie się bardziej przejrzysty, a popyt i podaż ulegną większemu rozproszeniu, co zbliży go do modelu rynku doskonale konkurencyjnego. Doprowadzi to do zwiększenia bezpieczeństwa wymiany, a tym samym zmniejszenia kosztów transakcyjnych. Celem niniejszego opracowania jest wskazanie wpływu technologii blockchain na kształtowanie się kosztów transakcyjnych, a także określenie czynników, które odpowiadają

za zwiększenie bezpieczeństwa wymiany z zastosowaniem blockchain, oraz wskazanie potencjalnych problemów związanych z tą technologią.

Słowa kluczowe: blockchain, gospodarka sieciowa, sieci peer-to-peer, wymiana rynkowa, koszty transakcyjne.

1. Introduction

The problem of ‘exchange safety’ has been interesting for economists for as long as the discipline has existed, and is of special interest to institutional economics and new institutional economics. The term ‘exchange safety’ refers to an array of conditions favourable to performing a market transaction, especially trust between the exchange participants and transparency of the exchange. One can assume that only a perfectly competitive market can be perfectly safe for a model where supply and demand are dispersed, the product is homogenous, the market can be entered and left freely and information is perfectly available. This perfect state is impossible in reality. However, the development of IT allows the exchange conditions to approach the perfect model. The rise of the Internet and the digitalisation of economic processes were the key factors here, and another important factor is the introduction of blockchain transactions.

Blockchain technology is known primarily through its use in cryptocurrency, but it can be used in a much wider field. The technology is based on peer-to-peer protocol, which means that it can be – and is – used for exchanging digital goods, or for transactions that use digital data, this means all the transactions registered by computer systems. The potential of this technology leads to the hypothesis that it may become the equivalent of the invisible hand of traditional market exchange, meaning primarily the autonomy of transactions that use it. Blockchain technology will make the market of the network economy more transparent, while demand and supply will become more transparent, which will bring it closer to a perfectly competitive market. The goal of this paper is to indicate the impact of blockchain technology on transaction costs, as well as to show the factors which increase exchange safety when using blockchain and to point out potential problems with this technology.

2. The nature of a network economy

A network economy is a term used to describe all the interactions between economic subjects that are made with the use of the Internet. While other computer networks do exist, this one is the most popular. The idea of a network itself is not new – according to Giddens networks have always been a part of the social order, but only the recent technological developments have made them ubiquitous (Giddens, 2012).

Every network has three qualities: it is elastic, scalable and viable. Castells claims that these three qualities determine the existence of a network society (2013). An elastic network can adapt to changes in its internal environment. For instance, if a given social networking service gains popularity, it no longer needs to work through a single node in the network, but can be distributed among many (servers, computation centres etc.). This allows avoiding overload, for instance. Scalability is a related term – a scalable network can change its size (through adding new nodes or overtaking traffic by other, existing nodes) without being disrupted. These two traits make a network viable, meaning that it keeps on functioning even if some of its nodes disappear. A network is a decentralised system (Castells, 2013).

Another characteristic trait of a network is its capacity for asynchronous interaction, meaning that the actions of economic entities within the network can take place at any time and place in the world. This allows for the existence of markets that never sleep and function twenty-four hours a day. Asynchronicity allows for exchange executed through any device connected to the network, in any place in the world and therefore independently from time zones. This term also means the possibility of delaying interactions (Brol and Czetwertyński, 2013) – if an offer to sell is on, then an offer to buy can come in at any time, outside the regular opening hours of a shop or any other selling entity. Any commercial contacts where the participants can negotiate at a time they choose can be made in this way.

In the modern network economy based on the Internet, the costs of accessing the network are low or even non-existent (of course, provided that we have adequate infrastructure and equipment). This does not mean the cost of the Internet providing service, but the cost of entering a given market or the cost of information transmission.

2.1. Peer-to-peer systems

Peer-to-peer systems are distributed software systems made of nodes (individual computers) which make their computing powers available directly to another node. Joining a peer-to-peer system, users turn their computers into nodes in the system, all of which are equal in credentials and roles. While users can differ by the resources they bring into the system, the nodes have all the same possible functionalities. Thus, all the computers are providers and consumers of resources.

In such a system there is no need for any intermediary between a producer of digital goods and their consumer. This fact is important because many items of everyday use are becoming digital. The best example here is the change in the music market. In 2017, global income from music streaming sales surpassed the income from selling music in traditional form (records, CD or vinyl). The income amounted to \$6.6 billion and \$5.2 billion respectively (Sweeney, 2018), and while intermediaries do still exist in this market (Spotify, Apple Music and others), the propagation of peer-to-peer technology made direct distribution possible for many artists not tied to any particular music publisher. This solution was pioneered by the band Radiohead, which decided to sell their music directly on the Internet already in 2007 (Kot, 2009).

A similar revolution occurred in the financial products market (banking services, loans, insurances etc.) and administrative services offered by e-administration platforms (in Poland, such as ePUAP, PUE, ZUS, CEIDG, eKRS, and many others).

2.2. Blockchain technology

A blockchain is an open source database, using the Internet and peer-to-peer architecture to register transactions. Its characteristic trait is decentralisation, meaning that it does not have one specific place to store its data, it is open, public, and coded with cryptography algorithms, which can be seen as a digital register book containing many entries. Its decentralised characters means that making new entries happens on many computers at once, which means existing entries cannot be changed. Each block contains a cryptographic summary of the previous block in the chain.

Distributed peer-to-peer systems can use a blockchain as a tool to keep their interactions ordered and transparent. A blockchain can therefore be considered a tool for keeping integrity in various distributed systems. Computer experts define blockchain technology as a “solution that maintains a continuously growing list of data records that are confirmed by the nodes participating in it” (Yli-Huumo, Ko, Choi, Park, and Smolander, 2016, p. 1); this means that the system is autonomous. Without a specific, central data storage spot, the data cannot be simply deleted. Its storage in many nodes – computers linked to a peer-to-peer network – prevents any data falsifying as well, since the usual practice is for a block of data (or even several blocks) discovered to differ from the majority to be rejected as faulty (Drescher, 2017). This shows the commercial potential of the blockchain technology, seeing as the “block” used here can mean one or many linked transactions (Singhal, Dhameja, and Panda, 2018). This fact in turn leads to the conclusion that an autonomous system of encrypted, linked transaction-blocks guarantees full exchange safety (Drescher, 2017).

For these reasons, the primary goal of the creator of blockchain technology was to issue a separate currency, the worth of which would be determined only by the existing amount of the currency and the demand for it, thus the Bitcoin cryptocurrency came into existence. It uses a distributed, encrypted registry system and is entirely virtual. The system works by creating nodes, called wallets, accessed only by a single user with their unique, encrypted key (cryptographic hash) (Nakamoto, 2009). The user thus controls the contents of the wallet in the same way they would control the contents of their actual wallet with cash. All the money flow of cryptocurrencies (there are currently many in existence, some of them with a large market capital) are registered by their internal algorithms.

3. Transaction costs

Trust is the key factor in decentralised markets with many agents (agents as described by the agency theory, describing the relationship between the authority and the plenipotentiary in an enterprise). Lack of trust generates costs – the costs of safeguarding the interests of the market exchange parties. Due to uncertainty, opportunism and incomplete information (the limited rationality of economic subjects), the lack of trust between agents limits the number of interactions and relationships created within market relations. Such barriers in creating bonds, resulting from lack of trust, were described extensively in the transaction cost theory (part of institutional economics) created by Ronald Coase in 1937 (Bheemaiah, 2017, p. 214).

Transaction cost theory (TCT) is a branch of economics dealing with transaction costs and the institutions created to manage those costs. It is particularly interested in the costs of economic relations and the ways in which agents organise dealing with market interactions. Coase realised that economic transactions create additional costs, and in his breakthrough article, “The Nature of the Firm”, pointed out that while economic process requires a great deal of planning, much of this planning is not coordinated by the market system and happens within a firm (Hidalgo, 2015). As firms have certain structures and hierarchies, most interactions within a firm have a political character. This results in an internal division of competences influencing the transactions and all interactions, and this in turn influences the final costs, which thus take shape outside the market mechanisms. Examples of such a situation include contracts, disputes, negotiations and other instruments which shape the exchange process. Their presence heightens the costs, and higher costs mean more resistance to a transaction (Bheemaiah, 2017, p. 215).

This idea was further developed by Williamson, who proposed a new approach to transaction costs, including an exchange of goods and money within companies. He claims that a transaction should be understood technically – as a delivery, which can occur both within a company and on the market. This definition of a transaction makes the costs of a company’s functioning to become transaction costs. A transaction occurs at any and every moment when the object of exchange changes hands. The amount of transaction costs incurred by a firm is a derivative of workload division (Hardt, 2005, p. 5). If overall trust between the cooperating sides is high, transaction costs are low. If a culture of mistrust persists between the sides, transaction costs are high.

Another analysis of transaction costs was developed by North. He concentrated on the transaction costs actually incurred, that is to say the costs of finding a transaction side, the costs of creating a contract, judiciary fees and the costs of insuring the transactions. Such costs result from an asymmetry in information distribution between sides. The buyer wants to obtain as much information as possible about the seller and their product, while the seller checks the credibility of the buyer (Hardt, 2005, pp. 14-15).

Trust is a necessary element of every network (in economics as a whole and in an individual enterprise) because it allows transferring information and knowledge. If trust within the network is greater, links are created with greater ease and transactions flow better, which expands the network. By lowering the link costs and offering better absorption of knowledge, high trust networks can adapt to changes in market and technology faster. This was described in detail by Hidalgo in his book entitled “Why Information Grows” (2015).

Blockchain in this case is a mechanism which allows enforcing the execution of agreed contracts through encryption. There is no need for a consensus between the transaction sides, because the technology offers a control mechanism which limits the need for trust by enforcing transparency (Davidson, de Filippi, and Potts, 2016).

4. Towards a perfectly competitive market

The way in which blockchain technology operates can be compared to a market intermediary, who helps to set the exchange conditions and enforces them. This digital intermediary is autonomous, independent, acting on a pre-programmed instruction scheme, and by encrypting the transactions as well as keeping track of if in many places at once makes deceit impossible. This allows the sides to make credible and irreversible transactions without third party participation. Contracts made with the use of cryptographic technologies are even called “smart contracts” although the term simply means a digital protocol for verifying and confirming a contract.

Over the last several years, the idea of “smart contracts” found its use in creating decentralised, autonomous organisations (DAOs). These are entities organised according to rules stated in a computer algorithm which is transparent, controlled by the participants and not subject to administrative influence or outside regulations. Such organisations can remain decentralised and function without the help of intermediaries testifying to transactions, such as notaries, central banks, acquiring banks, stock exchange etc.

An important trait of DAOs is lack of external regulations. This is also the case of cryptocurrencies. Every entity participating in the exchange, and every exchange conducted through the blockchain are subject to regulations defined in the already existing algorithm. In the case of Bitcoin, for instance, the following conditions apply:

- the “ledger” is digital and composed of many blocks,
- registration is carried out on many machines, preventing any changes to already registered blocks,
- each block contains an encrypted summary of the previous block in the chain,
- Bitcoin uses the proof-of-work system, in which the chain containing the most cumulated proof of transaction is considered the right one by the network,
- new blocks are created every 10 minutes.

DAOs function in a similar manner. This means that the exchange is decentralised, open, and public, coded with cryptographic algorithms and does not have a single

specific place of data storage (data is stored in the cloud). Once done, a transaction is not reversible.

The best-known enterprise of this type is the Colony system which provides a general purpose framework for the essential functions organizations require, such as ownership, structure, authority, and financial management. As the creators of this system claim on their website: “Colony is inspired by complex adaptive systems like ant colonies: dynamic networks of agents which react and adapt to stimuli from each other and their environment. From simple rules emerges collective behaviour and self-organization of the system as a whole” (Colony, 2020).

The qualities of blockchain technology bring transactions made with its use closer to the conditions of the perfectly competitive market, especially when it comes to transparency and supply and demand dispersion. This results in a diminished ability to influence the price on both sides of the market.

Shifting the exchange conditions towards perfect competition is associated with improved transaction security. There are several factors that can lead to this:

- automatic and autonomous nature of the exchange;
- no intermediaries;
- ease of processing and storing transaction data.

The first of these factors results from the specifics of blockchain technology discussed earlier. The autonomy of the exchange does not allow the possibility of external arbitrators influencing its course. Everything is done according to a specific, constant algorithm that is known to the parties to the transaction. Due to the block structure of the database and the use of cryptography, it is not possible to falsify records, which would require breaking the code and duplicating false entries in all the previously saved records.

The second factor is related to the elimination of the link, which can potentially affect the exchange process. Intermediaries are designed to improve the credibility and transactions through the powers given to them and possessed knowledge, where examples of such entities are: notaries, financial and insurance brokers, realtors, etc. In fact, their goals are the same as for all other economic entities – maximizing individual benefits, therefore they may act not as entities that facilitate the transaction, but distort it. In addition, their services are an additional cost, which through the possible embezzlement can be multiplied.

The third factor results from the ease of processing and storing large data resources in the cloud. Detaching from the place where transaction data is physically stored already increases security by itself. In addition, all records can be created in real time, and once created, records cannot be deleted.

All these factors enable the exchange to be carried out in a fully autonomous and much safer way than in “traditional” markets. Thus, despite the potential high costs of blockchain implementation, in particular those related to providing sufficient computing power, the benefits associated with savings resulting from lower transaction costs seem to be much greater than any cost.

5. Uses of blockchain in the economy

Up till now the main use for blockchain technology is found in cryptocurrencies, and this technology is strongly associated with them because it was first used there. However, blockchain can have many other uses, especially in financial services such as insurance, the stock market and banking.

The first bank to implement blockchain technology in Poland was PKO BP, which introduced a system that allows verifying the authenticity of bank documents. The solution used by PKO involves a medium (an electronic banking system) connected to a private blockchain network (available only to the users of the banking app) using Hyperledger Fabric technology. Documents are stored in an external archive with a trusted third party. The blockchain technology allows detecting changes made to a document by registering, in real time and in a distributed network, metadata (Distributed Ledger Technology) and the result of the cryptographic hash function.

This makes verifying documents less costly and take less time. That solution is only one of many possible uses of blockchains. A similar system can be made for any other banking procedure that is organised and repetitive, lowering the costs of operation of such entities. Since banking procedures, but also all other bureaucratic procedures, are binary, they can be replaced with a digital system. They have not been automated thus far mostly for safety reasons, but cryptography and distributed data storage, typical for blockchain technology, can allow for the autonomous handling of such procedures.

The distributed ledger technology mentioned above, is used for recording asset ownership. Currently, any transaction made by a commercial bank which results in ownership transfer, for instance of money or assets, must pass through a centralised system. Commercial banks keep a register of handled transactions in a local database, updated after a new transaction is made in the central system. A distributed ledger, on the contrary, is a transaction database that is not kept in a single place, but is distributed among many computers connected with a network. Usually, all members of the network can read the stored data and possibly add new data, depending on their credentials. The data are safe thanks to the algorithms, partly because any changes to stored data are visible to network members. This allows for greater effectiveness due to automated registering, eliminating human error and simplifying complex financial processes.

There are many other uses for blockchain technology outside financial services. It can be used anywhere where there are repetitive procedures, thus it can replace any kind of ledgers or registers, such as land registration systems, and eliminate intermediary agents who make changes to them. It can be used in logistics, ensuring supply chain transparency and reducing the costs of documenting it. Blockchain can be used in the public sector, eliminating the subjective aspect of clerical work and making the administrative system work faster.

Studies on the use of blockchain in the public sector mention the following areas in which this technology may find application: user registration, contract preparation and submission, bidding and selection, monitoring contract execution and auditing (Diallo, et al. 2018), therefore mainly in the field of public procurement and servicing of clients.

All these solutions have one trait in common – they lower transaction costs through shortening the time a transaction takes, ensuring transparency and limiting the number of people working on documenting and interceding in the transaction. The direct consequence is a safer exchange.

6. Limitations of blockchain technology

The use of blockchain technology does not eliminate all the safety issues and may generate new ones, cryptocurrency theft is an example here. According to information gathered by the F5 Labs organisation, which analyses data and makes reports on cybersecurity, the frequency and number of cryptocurrency thefts is rising.

Just in the first half of 2018, cryptocurrencies worth \$1.1 billion were stolen mostly through various attacks on the stock exchange, which represent 27% of all theft of this type. Other attacks include attacks on companies (21%), individual users (14%) and government institutions (7%) (Pompon and Vinberg, 2019).

There are several reasons for this. Firstly, there is a technology gap that results from lack of knowledge about the new technology on the part of new investors. In the same way that fiat money is supported by administrative and legal systems, cryptocurrencies require a social infrastructure. Any part of that infrastructure can be a target of attack, including wallet software, exchange platforms, blockchain algorithms that are the basis of the currency itself, and the people who use it. One of the emblematic examples of the cavalier attitude of users is the story of the Local Bitcoins discussion board, where criminals were able to establish the identity of six board users and use it to take over their wallets.

However, a real problem of the last few years are the fake cryptocurrency exchange markets. Profiting from the potential investors' lack of specialist knowledge, criminals created web services offering cryptocurrencies for sale and promised a large return on investments. In 2018 there were two spectacularly successful cases of such fraud – Purebit and Bitsane services which, in only the two months of their existence were able to amass around \$10 million (Pompon and Vinberg, 2019).

The huge interest on the part of investors is a contributing factor. Due to the frequently high profitability of cryptocurrency investments, the overall bulk of transactions is quite large, which led in several cases to theft executed by the staff handling client wallets or the exchange. This was the case of the Bithumb service robbed by one of the employees for the amount of \$19 million (Pompon and Vinberg, 2019).

The third limitation is the imperfect technical solutions used by the cryptocurrency exchange markets, sometimes verging to negligence. A service known as Gate.io Exchange leaked the individual, encrypted customer keys because of a gap in the software that gathered website statistics. This leak was discovered and neutralised in time, but a similar situation at Binance platform led to a loss of \$41 million (Pompon and Vinberg 2019).

Cryptocurrencies are an attractive target for attacks for other reasons as well. Many cyber thefts (password, data or database theft) provide thieves with illiquid assets – something that still has to be turned into money. Cryptocurrencies, on the contrary, are cash. The foundations of cryptocurrency are privacy, relative anonymity and autonomy, which may both help and hinder safety. Some of the same principles and tools that draw people to cryptocurrencies may also draw criminals to them.

7. Conclusion

Despite the risks indicated, blockchain technology seems to be an important step towards a better, more transparent and distributed market. One should expect a rise in number of transactions made with the use of blockchain technology, which will in turn lead to the technology becoming more popular and the technology gap between transaction parties being reduced.

Due to its decentralised structure, based on peer-to-peer architecture, blockchain databases cannot be hacked because they do not have one single, real address. They are also fully autonomous because they operate on the basis of an independent, automated algorithm. This in turn means they are fully transparent, since the transaction register is available to the public, and anonymous, since user identities are hidden by individual and unique cryptographic keys.

These factors all lead to better market transparency when using blockchain for transactions, and since these transactions are made on the Internet there are no market entry and exit barriers, which means supply and demand is dispersed. This in turn leads to lower transaction costs and better exchange safety. This conclusion concerns the situation in which economic entities already have access to the network and actively operate in it, otherwise, however, they have to take into account additional barriers. This can be a nuisance, in particular in a so-called “digital exclusion problem”.

References

- Bheemaiah, A. (2017). *The blockchain alternative. Rethinking macroeconomic policy and economic theory*. New York: Apress.
- Brol, M., and Czetwertyński, S. (2013). Grupy interesów w społeczeństwie sieciowym. *Prawo i Ekonomia, XII* (2), 313-324.
- Castells, M. (2013). *Władza komunikacji*, Warszawa: Wydawnictwo Naukowe PWN.

- Colony. (2020). About the Colony Vision. Retrieved from <https://colony.io/about>
- Davidson, S., de Filippi, P., and Potts, J. (2016). *Economics of blockchain*. Public Choice Conference, Fort Lauderdale.
- Diallo, N., Shi, W., Xu, L., Gao, Z., Chen, L., Lu, Y., Shah, N., Carranco, L., Le, T. C., Bez Surez, A., and Turner, G. (2018). *eGov-DAO: a better government using blockchain based decentralized autonomous organization*. Fifth International Conference on eDemocracy & eGovernment (ICE-DEG), Buenos Aires.
- Drescher, D. (2017). *Blockchain basics*. New York: Apress.
- Giddens, A. (2012). *Socjologia*, Warszawa: Wydawnictwo Naukowe PWN.
- Hardt, L. (2005). Instytucje a koszty transakcyjne w nowej ekonomii instytucjonalnej. *Gospodarka Narodowa*, 1-2(161-162), 1-19.
- Hidalgo, C. (2015). *Why information grows: the evolution of order, from atoms to economies*. Philadelphia: Basic Books.
- Kot, G. (2009). How Radiohead's business model shook up the music industry. *Chicago Tribune*. Retrieved from <https://www.popmatters.com/93659-how-radioheads-business-model-shook-up-the-music-industry-2496023949.html>
- Nakamoto, S. (2009). *Bitcoin: a peer-to-peer electronic cash system*. Bitcoin.org. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- Pompon, R., and Vinberg, S. (2019). *Cryptocurrency hacks 2019*. F5 Labs. Retrieved from <https://www.f5.com/labs/articles/threat-intelligence/cryptocurrency-hacks-2019>
- Singhal, B., Dhameja, G., and Panda P. S. (2018). *Beginning blockchain*. New York: Apress.
- Sweney, M. (2018). Slipping discs: music streaming revenues of \$6.6bn surpass CD sales. *The Guardian*. Retrieved from <https://www.theguardian.com/technology/2018/apr/24/music-streaming-revenues-overtake-cds-to-hit-66bn>
- Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K. (2016). Where is current research on blockchain technology? A systematic review, *Plos One*. Retrieved from <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477>