CHALLENGES AND OPPORTUNITIES OF BLOCKCHAIN TECHNOLOGY REGULATION

Sonja Bunčić [1] [ORCID 0000-0002-0867-585X], *Milica Njegovan* [1] [ORCID 0000-0002-3651-5714]
[1] *University of Novi Sad, Faculty of Technical Sciences, Department of Industrial Engineering and Engineering Management, Novi Sad, Serbia*

Abstract: *Accelerated technological development has brought many novelties, among which is distributed ledger technology (DLT), often called blockchain (BC). BC is perceived as a peer-to-peer distributed immutable ledger that could revolutionize economies, societies and even our daily lives. All protocols for dealing with data and transactions are coded with an algorithm, so there is no need to trust the other contracting party or the intermediary. With the concept of decentralization and the absence of hierarchy, BC wants to avoid all traditional intermediaries and any regulation. The question arises, are BC-technologies really decentralized and who controls them? What are the consequences if decision-making in BC is influenced by small groups of people or corporations? This article, in an attempt to answer these questions, explores technological scandals in which there have been significant deviations from the basic principles of BC (The DAO Hack, Parity's Smart Contract Bug on Ethereum and Facebook's Libra). Analysis of the above scandals suggests that decentralization is threatened and the current regulatory status of BC is substandard. It was shown that BC technology, due to its deterministic nature, cannot provide solutions for all life situations and that human judgment is irreplaceable.*

Keywords: *Blockchain technology, regulation, technological scandals*

1. BLOCKCHAIN TECHNOLOGY – DEFINITION AND CHARACTERISTICS

Blockchain technology (hereinafter: BC) is a product of accelerated digital development. BC is perceived as a peer-to-peer distributed immutable ledger that could revolutionize economies, societies, and even our daily lives. Although it is already widely used, BC still represents an insufficiently clear technology for the general public, so it is necessary to describe it more closely. It is about distributed ledger technology (hereinafter: DTL). This means that the data is recorded simultaneously on all computers in the network, and not in one, central place. In principle, the validity of new transactions or authorized data transfer is not approved by one central point, such as central ledger, but by the network participants themselves, using the consensus protocol. After approval, transactions are recorded as a new changed state of data on the BC, which is visible as such to network participants. In short, it is a concept based on the use of a cryptographically protected chain of transaction blocks through a "hash" function, which further means that the content of the block cannot be changed without changing the content of all other blocks that precede it (Cvetković, 2020:128). The verification and consent processes are fully automated. All protocols for handling data and transactions are coded with an algorithm (Shein, 2019).
The principles on which the BC technology system was originally founded are different from traditional systems, for which it is crucial to have a central administration (which makes decisions on behalf and for the account of the members), so an intermediary relationship is established there. A characteristic of BC (unlike traditional systems) is that it is formed as an equal, all participants have the same status, which is the result of solid coding, and it is not even necessary to have trust in the other contracting party, i.e. in the intermediary (Čulinović-Herc, 2022:698-699). The concept of decentralization in record-keeping and the absence of control by a central body aims to bypass traditional intermediaries, such as regulatory agencies, central banks (Nakamoto, 2008), as well as the establishment of a code of conduct and to avoid the adoption of any legal regulations.

1.2 Features of Blockchain tehnology

The characteristics of BC, in addition to equality and independence in relation to traditional systems, also include technological elements such as: immutability, data verification and decentralization.
Immutability, as a technological characteristic of BC, arose from the fact that in the blockchain chain there are several network participants (computers), and they are responsible for ensuring the accuracy of the data. In traditional transactions, unknown intermediaries and unknown participants (computers) do

not trust each other about the accuracy of information. Unlike traditional institutions (banks, government institutions and similar authorized intermediaries) responsible for maintaining and controlling such records, blockchain is designed to be immutable. Each record (as part of a unique block) entered into the blockchain is secured by a unique cryptographic key (Makoto Yano, 2020:3-4).
Data verification in BC is related to the ability to store and share information through blocks in a peer-to-peer network. Identical copies of blocks (which are functionally record-keeping inserts) are jointly verified by members of the network, using the consensus method. The verified information is contained in blocks that have been added to the chronological chain of existing and approved blocks using a cryptographic signature. Essentially each block has loaded data about all previous blocks (transactions) within one blockchain. The importance of BC technology is that it ensures the authenticity of digital data: trust in the classical legal relationship is replaced by verification through data in blocks in the above mentioned way. BC concept is transparent and enables efficient (fast and cheap) transmission of information in wide IT networks (Cvetković, 2020: 129).
Decentralization is a key characteristic but also the biggest challenge of BC because it is global in terms of the composition of participants, and cross-border in terms of the nature of transactions. The initiator of the BC is the first potential addressee of the regulation, but since he no longer has control over it after "commissioning the BC", it is not pragmatic to impose regulatory requirements on him. It should be kept in mind that the BC network may be technologically decentralized, but that legally and factually one person controls the network because he has the computing power needed for network consensus (Čulinović-Herc et al., 2021:330).

1.3 Types of Blokchain technology systems and decision-making methods

BC systems differ from each other according to various criteria, whether public or private, with or without permission, and in terms of achieving consensus. BC is public when anyone can access it and use it to conduct a transaction, i.e., private (or semi-private) when only a limited and predetermined number of participants can access the system (e.g., only banks and insurance companies). Further, BC can be divided into "permissionless" and "permissioned", depending on who can execute transactions and who can verify them. If anyone can execute and verify transactions, it is a permissionless BC. If authorization is required to execute or validate transactions, or both, the BC is called permissioned (Čulinović–Herc, 2022: 159).
BC, as we stated, promises, on the principles of democracy and immutability, safety and independence of participants, guaranteeing traffic on a well-programmed algorithm. With the concept of decentralization and the absence of hierarchy, BC wants to avoid all traditional intermediaries and any regulation. The question arises, are BC-technologies really decentralized and who controls them? What are the consequences if decision-making in BC is influenced by small groups of people or corporations? These questions arose in cases where the programmed algorithm led to unexpected problems and the need to make a decision on the further fate of BC participants. The decision about it is most often made by influential members of the BC-community, that is core developers. In BC-systems that are based on access approval, that is, which are not public, it is somewhat logical because that BC remains in the control zone of the entity that established it and opened access to the network only to selected individuals. However, key developers have an equally important influence in public BC. Their behavior is not regulated by regulations, ethical rules or rules of conduct, and this represents a potential risk.

2. TECHNICAL SCANDALS THAT SHOOK THE BC COMMUNITY

The technical scandals that we will present in the following part of the paper show that even BC systems are not perfect and that they need human intervention. In that case, the decision made should be without the influence of subjective factors (conflict of interest, political influence, etc.), and as a rule, it must be adopted according to the same rules of procedure.
In the paper, we used a descriptive method followed by an analysis and a synthetic method to prove our hypothesis that BC systems are not perfect and that they need human intervention without the influence of subjective factors.

2.1 Attack on The DAO and Implementation of a "Hard Fork"

A Decentralized Autonomous Organization (DAO) is a set of smart contracts (Neitz, 2019:18) on the *Ethereum* BC network, on which the cryptocurrency called *ether* is traded. Smart contracts are computer protocols that execute, monitor and/or document legally relevant actions (especially the execution of contractual obligations) conditioning them on digitally confirmed results. A smart contract differs from a classic contract in that it is self-executing, i.e. obligations are fulfilled with little or no human activity. Their concept was created by lawyer and cryptographer Nick Szabo in 1994, and he described them as computerized transaction protocols that execute the terms of a contract (Szabo, 1994). Immutability, i.e., unstoppability of smart contracts is both their advantage and disadvantage. The DAO in question was founded in 2016 to enable the financing of startup projects in a joint virtual organization Garcia (Rolo, 2019). Jentzsch, a theoretical physicist, came up with the idea that crowdfunding for startups is not carried out for each new one separately, but through investments in DAOs. The DAO was the one who invested those funds in startups or projects by selecting the token holders in the DAO, i.e. its members. During the DAO's initial token offering in May 2016, around USD 150 million worth of virtual currency was raised, breaking the record for funds raised through crowdfunding. However, on June 16, 2016, there was an attack on the DAO due to the existence of certain flaws in its code. Namely, the code had a programmed, so-called protection of the minority. Token holders who would vote against a project accepted by the majority could initiate a split of the DAO. A minority could transfer their tokens/ethers to a new DAO (further: DAO child) which was subject to the same rules as the initial DAO (Karapetsas, 2016). But the partition protocol was hard-coded.

In other words, after the DAO split process started, it took at least 48 days for the virtual currency to "sit on the account" of the split initiator. The attacker took advantage of flaws in the coding of the protocol. After activating the DAO split function, the code would first mark the tokens/ethers, which will pass to the child DAO, but did not simultaneously update the account balance of the initial DAO. In addition, the code did not protect the sharing protocol from, so called recursive call. It is a term used to refer to a function that "calls itself". The attacker was able to "recursively call" the split function and retrieve the funds multiple times before the split hodogram reached the point where the code itself checks the ether balance of the DAO account. By abusing a recursive call, on June 16, 2016, the attacker managed to appropriate about 3.6 million ethers from the DAO, which was approximately a third of the entire DAO's assets. After the announcement of the event, the value of ether almost halved. So, two factors made the attack possible. The code was not protected against recursive calls, and the smart contract was not programmed to update the balance at the same time as the currency was sent. Basically, it's about coding flaws.

An intense discussion ensued in the BC community about what needed to be done. The attacker published an open letter to the ethereum community (Gautham, 2016), claiming that the misappropriation was not illegal because the code was legal. He considered that it was not legitimate to consider his transaction null and void because everything was acquired precisely according to the terms of the smart contract. Due to the split protocol explained above, the BC community had 27 days to decide on how to recover the system from the attack before the attacker initiated a proposal to transfer ether to their account (Güçlütürk, 2018). The community considered the application, the so-called "soft or hard forks", as well as whether to do anything at all. A "soft fork" would mean that all (future) transactions, which would withdraw funds from the DAO, would be considered void. Transactions that took place before the soft fork were applied would be valid. A "hard fork" would erase the history of all DAO transactions since the beginning of activity.

Opponents of both solutions relied on the philosophical underpinnings of the ethereum blockchain. They claimed, like the attacker, that "the code is the law" and that everything the code allows is legitimate. The application of a "hard fork" threatened the principle of record immutability as one of the most important features of BC.

Key developers proposed a soft fork vote that began on June 22, 2016. The decision was made by a majority and was supposed to be implemented on June 30, 2016. However, due to additional security flaws, the "soft fork" was abandoned (Güçlütürk, 2018). After that, the discussion about the "hard fork" began. It was argued that the attack was too serious to ignore. The decision to implement the "hard fork" was voted and accepted by the majority of miners (eng. miners) of the ethereum community. The "hard fork" was completed on July 20, 2016, and the funds were returned to investors (del Castillo, 2016). According to some authors, this decision was imposed by seven key developers. Thus, a new version of the Ethernum network was formed, with different rules from the original ones.

From this example, it is evident that the BC community deviated from the basic technological settings of BC (code = law). The decision was made under the influence of key developers. On the other hand, the decisions that were voted once were abandoned in the execution procedure ("soft fork"), which shows serious deficiencies in the management system and the way of decision-making in the BC community.
This event certainly raised doubts about the BC technology and started a discussion about the need to regulate it. It is noticeable that human decision proved to be irreplaceable, although all problems should have been foreseen and solved in smart contracts.

2.2 Parity Contract Bug

Parity is a trading company founded by Gawin Wood (otherwise the co-founder of Ethereum) together with the Ethereum Foundation's DEV team. They were also the authors of the Solidity program for programming smart contracts. Parity developed the so-called wallet with multiple signatures (multi-sig wallet). The characteristic of this wallet is that the transaction requires the use of two or more private keys, which is more secure than one. The vulnerable MultiSig wallet was split into two contracts to reduce the size of each wallet and save gas: A library contract called "WalletLibrary" and an actual "Wallet" contract consuming the library (Breidenbach et al., 2017). Parity was accidentally exposed to a bug in smart contracts, which allowed one user to unilaterally change the owner names and usage parameters of other people's wallets that contained 150 thousand Ether (Parity Technologies, 2017). This allowed an attacker to make himself the owner of three wallets and transfer ether from those wallets to wallets under his control. Around the same time this happened, a group of white hat hackers exploited this flaw and made themselves to the owners of the next 593 wallets, which had more than 377 thousand ether, only to have the wallets returned to their rightful owners after Parity fixed the problem. But in eliminating that problem, an even bigger mistake was made. It was noticed that the new, improved smart contract was not activated, and during its activation, the beginner, employed at Ethereum, first made himself the owner of the entire library of smart contracts. By controlling the library of smart contracts, control was also established over all multi-sig wallets. Therefore, the activation of the new program led to the freezing of 584 wallets with more than 500 thousand ether. In order for the wallets to be returned to their rightful owners, a hard fork had to be applied again, which the injured wallet owners advocated for. However, the key developers rejected that possibility, and the ether currency remained permanently frozen on those wallets.
In this scandal too, we see that in case of errors in smart contracts related to BC, the decision on the fate of "equal" participants is made by only a few key developers. In addition, it is noticeable that in these two unprecedented technical scandals, the same measures were not applied to eliminate deficiencies, which is a deviation from the original principles of BC.

2.3 Facebook Libra and forced moratorium

On June 18, 2019, the Internet giant Facebook announced the creation of a consortium of financial and technology companies aimed at establishing a global cryptocurrency with stable value called Libra. It is planned to create an open blockchain through a new programming language, which will serve development teams in the future for creation of smart contracts. Just a few hours after the announcement that BC will be used for a new global cryptocurrency, the US Congress issued a statement. Financial Services Committee Chairwoman Maxine Waters demanded a moratorium on Facebook's further steps until Congress and regulatory bodies examine the announced Libra project.
The attempt to further develop BC technology (by creating a global cryptocurrency) based on the original principles seems to have posed a great danger to the real world, and the political influence of one of the strongest financial powers was used to stop Facebook's announced project. Therefore, even in the Facebook project, the decision on its further development was made outside the BC community, under the influence of politicians.

3. DISCUSSION AND CONCLUSION

The implementation of the “hard fork” in the case of the DAO attack and the lack of its implementation in the case of Parity are examples of the large influence of a small number of key developers in attack situations. It turned out that different decisions were made in similar cases. This creates a state of high legal and ethical uncertainty. Were the key developers in the first case biased and protected investors "from trusting them" or maybe they insisted on implementing a hard fork because they themselves were

affected by that attack? How does this reconcile with the basic principle of permanence and immutability of records at BC and of decision-making in a participatory manner? Not only was the code changed, but the basic principles on which BC-technology rests were called into question.
The above-mentioned questions show us that BC management has not moved far from management in a traditional way because a significant part of the decision-making process is not explicit, and the users are not completely independent. In the case of Facebook, there is an obvious political influence from which BC, by its very nature, wants to distance itself, and as it is evident, it is not able to resist it with its original principles. The decision-making and management procedure of BC technology, in all three mentioned cases, indicates that the idea of participatory democracy, which is important for BC, has been abandoned. If the management of a public BC is so strongly influenced by a small number of influential persons, those persons are bound to embed their biases and conflicts of interest in the network (Werbach, 2018:528-529).
The analysis of the mentioned technical scandals indicates numerous shortcomings in the automatic management of BC technology, i.e. that they require human reaction and decision. At the same time, it is evident that there are no established rules of conduct or legal responsibility of influential members who make decisions related to the entire BC. It would be necessary to start adopting ethical principles in the decision-making system of BC, as a step towards later legal regulation, which would regulate and ensure the management of potential conflicts of interest arising from the fact that decisions about changing the code are made by people.

4. REFERENCES

Breidenbach, L., Daian, P., Juels, A, Gün Sirer, E. (2017) *An In-Depth Look at the Parity Multisig Bug*. Available from: https://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/ [Accessed 15th july 2023]

Cvetković, P. (2020) Blokčejn kao pravni fenomen: Uvodna razmatranja. *Zbornik radova Pravnog fakulteta u Nišu.* 59 (87), 127-144. Available from: DOI: 10.5937/zrpfn0-24414

Čulinović-Herc E. (2022) Zlouporabe blockchain tehnologije i utjecaj na trgovačka društva, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci.* 43 (3), 697-716.

Čulinović-Herc, E., Zubović, A. & Derenčiković, M. (2021) Blockchain Tehnologija-prema novom regulatornom okviru za tokenizirane vrijednosne papire. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*. 42 (2), 323-341.

del Castillo, M. (2016) *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*. Available from: https:// www.coindesk.com/tech/2016/07/20/ethereum-executes-blockchain-hard-fork-to-return-daofunds/ [Accessed 14th july 2023]

Garcia Rolo, A. (2019) Challenges in the Legal Qualification of Decentralised Autonomous Organisations (DAOs): The Rise of the Crypto-Partnership? *Revista de Direito e Tecnologia*. 1 (1), 33-87.

Gautham. (2016) *DAO Hack, Attacker Sends Open Letter to Ethereum Community*. Available from: https://www.newsbtc.com/news/dao-hack-attacker-sends-open-letter-to-ethereumcommunity/ [Accessed 15 july 2023]

Güçlütürk, O. (2018). *The DAO Hack Explained: Unfortunate Take-off of Smart Contracts*. Available from: https://ogucluturk.medium.com/the-dao-hack-explained-unfortunate-take-off-of-smartcontracts-2bd8c8db3562 [Accessed 18th july 2023]

Karapetsas, L. (2016) *How to split the DAO*. Available from: https://github.com/slockit/DAO/wiki/Howto-split-the-DAO [Accessed 10th july 2023]

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available from: https://bitcoin.org/bitcoin.pdf [Accessed 25th june 2023]

Neitz, M. (2019) The Influencers: Facebook's Libra, Public Blockchains, And the Ethical Considerations of Centralization. *North Carolina Journal of Law & Technology.* 21 (2), 40-70.

Parity Technologies. (2017) *The Multi-sig Hack: A Postmortem*. Available from: https://www.parity.io/blog/the-multi-sig-hack-a-postmortem [Accessed 10th july 2023]

Shein, E. (2019) *How Blockchain Changes the Nature of Trust*. Available from: https://www.linuxfoundation.org/blog/blog/how-blockchain-changes-the-nature-of-trust [Accessed 15th june 2023]

Szabo N. (1994) *Smart contracts*. Available from: , https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart. contracts.html [Accessed 5th july 2023]

Werbach, K. (2018) Trust, but Verify: Why Blockchain Needs the Law. *Berkeley Technology Law Journal*. 33 (2), 487-550.

Yano, M., Dai, C. H., Masuda, K., Kishimoto, Y. (2020) Creation of Blockchain and a New Ecosystem. In: Yano, M., Dai, C. H., Masuda, K., Kishimoto, Y. (eds.) *Blockchain and Crypt Currency*. Springer Open, Tokyo, Japan, Economics, Law, and Institutions in Asia Pacific, pp. 1-19. Available from: https://library.oapen.org/bitstream/handle/20.500.12657/37713/2020_Book_BlockchainAndCryptCurrency.pdf?sequence=1 [Accessed 5th july 2023]