Preliminary communication UDC 17.022(045)
doi: 10.21464/sp35209
Received: 31 July 2019

Jurica Marković
Ministry of Defence of the Republic of Croatia, Trg kralja Petra Krešimira IV br. 1, HR–10000 Zagreb
jumarkovic@gmail.com

Ethical Foundation of the Blockchain Technology – an Introductory Inquiry

Abstract

This article briefly examines the blockchain technology, addresses the core ethical issues concerning its implementation, and considers its current and potential social role. During the research, virtue ethics revealed itself to be most compatible for understanding and describing the technical fundaments of blockchain and the scope of its application.

Keywords

blockchain, technology, ethics, virtue ethics, cryptocurrency

1. Defining the Blockchain Technology*

1.1. Working Definition

The blockchain technology is a decentralised peer-to-peer[1] system of computer network which enables a direct transfer of data between nodes,[2] thereby eliminating the need for third parties.[3] All transactions that take place in such

*
This paper is an updated and revised research based on the masters thesis "Ethical Foundations and Moral Challenges of Blockchain Technology", successfully defended at the Faculty of Humanities and Social Sciences of the University of Zagreb in 2018.

1
Alex Tapscott, Don Tapscott, "A cautionary tale of the blockchain regulation", para. 6, in: Alex Tapscott, Don Tapscott, The Blockchain Revolution, Brilliance Audio, 2016 [Microsoft Edge, EPUB format]. Note that in this paper the term blockchain will be used in the particular sense of decentralised system of peer-to-peer computer network with the distributed ledger. The entire section of this paper is based on that premise, and every subsection holds logical implications based on that premise (which mainly includes subsection 1.1.5. on how the blockchain system operates). As of 2018, there is a constant urge to enhance blockchain technology, and new concepts of blockchain systems continuously emerge. For example, centralised blockchain with a distributed ledger or decentralised blockchain with a limited ledger. Therefore, it is possible that the chosen model for this paper is not the optimal operating model. Some authors predict mainstream usage of blockchain technology in 2021 and its maturing for a day-to-day usage in 2025. Cf. Imran Bashir, *Mastering Blockchain*, Packt Publishing, Birmingham 2018, p. 10. For some examples, consider Voatz for electronic voting (https://voatz.com/), Everipedia, a blockchain encylopaedia (https://everipedia.org/), Paxos dedicated to brokering solutions (https://www.paxos.com/), and Northern Block for supplying solutions (https://www.northernblock.ca/products-supply-chain-provenance).

2
The node represents the computer whose end user is a human being. – A. Tapscott, D. Tapscott, "Networked integrity", para. 4 [Microsoft Edge, EPUB format].

3
Ibid., "Distributed power", para. 6 [Microsoft Edge, EPUB format].

a system are recorded in the distributed ledger[4] and coded as concatenated blocks,[5] thus giving rise to the term *blockchain* technology. This technology was devised to build and maintain trust and integrity[6] as a means of ensuring security. There are two kinds of technology which are involved in this process: hash technology and cryptographic technology.[7] While the blockchain technology has a wide and ever-expanding range of applications, it is currently best known for being used to facilitate cryptocurrency transactions. The term *blockchain* refers to four[8] distinct concepts:

1. Data structure: in computer science and software engineering, a *data structure* is a way of organising data regardless of their actual information content.
2. Algorithm: in software engineering, the term *algorithm* refers to a sequence of tasks that need to be executed by a computer.
3. Set of technologies: the term *blockchain* can be used to refer to a combination of concepts such as blockchain data structure, blockchain algorithm and various cryptographic and security technologies which can be used to ensure integrity in a purely distributed peer-to-peer system, regardless of its use.
4. An umbrella term for purely distributed peer-to-peer systems with a common area of application, as well as an umbrella term for purely distributed peer-to-peer systems of ledgers which use the blockchain technology package.

In this paper, I described what is understood by 1) and 2) while adhering to 3), and I also mentioned 4) when describing the application of the blockchain in the domain of cryptocurrencies. Also, it should be noted that the research presented in this paper is based on the *permissionless* blockchain system.[9] When discussing the blockchain technology, one must keep in mind that this is a newly emerging technology. The mechanisms behind the blockchain technology are continuously undergoing development. As a consequence, a robust definition of what constitutes the blockchain technology is yet to be offered. The possibilities of its application and the ramifications it may produce are likewise under constant consideration.

1.2. Decentralised System of Peer-to-Peer Computer Network

Two main architectonic solutions of a computer system are centralised and decentralised software system. In a centralised software system, components are connected around the central component, whereas in a decentralised system, there is no central component responsible for coordinating or controlling other system components.[10] *Blockchain* technology is based on the decentralised system as a tool for building and maintaining *trust* and *integrity*. *Integrity* is a non-functional aspect of a system with the purpose of gaining security, completeness, consistency, accuracy and absence of errors and corruption. *Trust* is faith, within a specific relationship, in reliability, truthfulness or skills of another without any proof or inquiry. Trust is given beforehand and can increase or decrease according to the interaction.[11]

In the case of the system of peer-to-peer network of computers, the nodes are peer-to-peer when it comes to coordination and supervision over each other. There are no superior and inferior nodes in such a system. However, the data and information in this system are distributed amongst all the nodes, and the question arises regarding how to gain integrity and trust within the system,

without the central authority that would give orders on how this should be executed. The problem can be even more exacerbated with the question regarding how to gain integrity and trust in the decentralised system of peer-to-peer computer network, where we are neither familiar with the exact number of nodes nor is it known how much trust can be put in the other nodes. In fact, I shall assume the worst possible scenario and say that we cannot have any trust or reliability in any node within the system whatsoever. This problem had arisen before conducting this study. It can be found in the literature under the term *problem of the Byzantine generals*.[12] To resolve these issues, one must examine the technical setup of *blockchain* technology. A solution to the problem of the Byzantine generals has been offered, and it lies in two technological components of blockchain – hash value and cryptography.

1.3. The First Technological Component: Hash Value

Hash values are produced by bits and bytes that constitute data. To transform data into the number of fixed lengths,[13] we would need so-called *hash functions*. These functions are computer programs that enable the transformation of any data (regardless of the size of the input) into the number of fixed lengths. What is important for this paper is the specific group of hash functions that are called *cryptographic hash functions*. They are specific because they can produce a kind of "digital fingerprint" for any input.[14] A hash value

4
Ibid., "How this worldwide ledger works", para. 1–7 [Microsoft Edge, EPUB format].

5
Daniel Drescher, *The Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress, Frankfurt am Main 2017, pp. 111–122.

6
Cf. ibid., pp. 29–32.

7
Cf. ibid., pp. 70–79, 93–101.

8
Cf. ibid., pp. 34–35.

9
Robert Herian, *Regulating Blockchain*, Routledge, New York 2019, p. 18. Herian mentions that there are permissioned, permisionsless and hybrid blockchain systems.

10
D. Drescher, *The Blockchain Basics*, p. 11.

11
For the term trust cf. William Mougayar, Vitalik Buterin, "A New Trust Layer", para. 1–10, in: William Mougayar, Vitalik Buterin, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, John Wiley & Sons, Hoboken, New Jersey 2016 [Microsoft Edge, EPUB format]; Paul Vigna, Michael J. Casey, "Bringing 'Trustless' Software to Communities of Trust", in: Paul Vigna, Michael J. Casey, *The Truth Machine – the Blockchain and the Future of Everything*, St. Martin's Press, New York, 2018 [Freda, EPUB format].

12
"Related computation challenge is so-called problem of the Byzantine generals." – Melanie Swan, *The Blockchain: Blueprint for a New Economy*, O'Reilly Media, Inc., Sebastopol, California 2015, p. 2.

13
"Fixed length means having a set length that never varies. In database systems, a field can have a fixed or a variable length. A variable-length field is one whose length can be different in each record, depending on what data is stored in the field. The terms fixed length and variable length can also refer to the entire record." – Vangie Beal, "Fixed length", *Webopedia*. Available at: https://www.webopedia.com/TERM/F/fixed_length.html (accessed on 10 September 2020). Cf. Eric W. Weisstein, "Hash Function", *MathWorld*. Available at: http://mathworld.wolfram.com/HashFunction.html (accessed on 10 September 2020). Cf. I. Bashir, *Mastering Blockchain*, p. 106.

14
Cf. Roger Wattenhofer, *The Science of the Blockchain*, Inverted Forest Publishing, 2016, p. 80.

is, in itself, unique as is the fingerprint of a person and it is therefore impossible that there exist two fingerprints in a collision.

Additionally, cryptographic hash functions are pseudo-random. It is impossible to predict *hash* values based on the input.[15] To simplify – if we try to gain *hash* value from the same input, then the *hash* value will always alter and be different in every attempt. Another distinctiveness of cryptographic *hash* values is that, through them, we cannot trace the original input that produced the specific hash value. This makes cryptographic hash functions unidirectional functions. When we create a particular hash value, we apply the hash function to the specific data. This process is called *hashing*.[16] Besides the term *hashing*, I will mention the term *hash reference*. Hash references relate to the data that is stored somewhere else, for example, on a hard disk or in a database. Hash reference enables the connection between the cryptographic hash value and the information on the exact location of a particular data in the system (when we talk about the blockchain, it implies the decentralised system of peer-to-peer computer network). If data in the system is altered, the hash value of this data and the information on the exact location of the data in the system becomes invalid. As hash reference relates to (refers to) the exact location of a data in the system and its hash value, hash reference itself becomes invalid.[17]

1.4. The Second Technological Component: Cryptography

Hash values protect the data in the blockchain technology with their technical characteristics. It could be stated that the second technological component in blockchain serves as an additional safeguard that protects the data and the end-users within the system. Through cryptography we aim to achieve security of all the users during sending and receiving certain data in the same system. It is crucial to protect the ownership of the user in both operations. At the same time, it should be noted that here blockchain technology has been put on a proper test because its challenge is to protect the personal property of every node (which represents the technological extension of every end-user), and, simultaneously, enable new interested users to enter into the decentralised system of peer-to-peer network of computers. Thus cryptography is a component that enables the identification of the users within the blockchain and the protection of their ownership.

Experience has shown that it is not desirable to have the same key for both encryption and decryption. By developing two different keys for the two processes, the asymmetrical cryptography is being created. This type of cryptography is used in blockchain. In the asymmetrical cryptography, the same key with which a certain text was created can never and under no circumstances be used for decryption of previously encrypted data. The encrypted data is also-called *cyphertext*. The two keys that we established exist in the domain of the asymmetrical cryptography are called *private key* and *public key*.[18] The private key can be used solely by the owner, while the public key is provided to everyone for potential use.[19] I will use the example of a mailbox[20] to make it easier to understand the problem.

Everyone can put the mail into the mailbox, but only the owner, with his own key, can unlock the mailbox and take his mail. A similar principle is used in blockchain technology. Anyone within the system can send the data to the owner of a certain node, but only the owner can decrypt the data with his unique key and gain insight into them. Such public-private access can suc-

cessfully identify the users, i.e. senders and receivers of certain data in the blockchain system and perform the data exchange between them. For the user to receive certain data within the decentralised system of peer-to-peer computer network with established blockchain technology, it is sufficient that he uses the private key and decrypts the data that had previously been encrypted by the sender while sending them to the system. However, to be able to send the encrypted data to the system in the first place, the sender must authenticate them by the digital signature. In this way, the blockchain technology ensures that only the true owner can transfer its ownership to someone else.

When we want to send our ownership (i.e. the data) to some other node, we use a unique digital signature. We can compare digital signature to personal signature in the real, physical world. When we use the digital signature, we place the encryption by the private key into a certain cyphertext (derived from the hash value of certain data). In that way, the creator of this digital signature can be traced through exactly this private key. Since it is actually about the hash value (that is also unique), we can clearly and precisely determine not only which data was sent but also in which point in time. When any user puts their digital signature on the certain data that they had intended to send to another node in the system, all the other nodes in the system can verify that data. All the other nodes detect certain data in the system by the principle of automatism and calculate their hash value. As user also enclosed the public key, all the nodes within the system using the public key decrypt the attached cyphertext that accompanies the sent data. Subsequently, all the nodes compare their initial calculations of the hash values of the sent data and the attached decrypted cyphertext, and if the results are the same, it can be stated that it is the *unique* digital signature of that particular user.

"Due to the fact that cryptographic hash values can be considered digital fingerprints, they are unique for each transaction. A constituting property of public-private-key cryptography is that cypher text created with one key can only be decrypted with the corresponding key. The association of both keys is unique. Hence, a successful decryption of cyphertext with a specific public key serves as a proof that it was created with the corresponding private key."[21]

15
D. Drescher, *The Blockchain Basics*, p. 73.

16
Cf. Narayan Prusty, *Building Blockchain Projects*, Packt Publishing, Birmingham 2017, p. 27.

17
"You create the cryptographic hash value of the data that are supposed to stay unchanged. When you need to verify whether the data were changed at a later time, you create the cryptographic hash value of the data again. You then compare the newly created hash value with the hash value that was created in the past. If both hash values are identical, the data were not changed after the first hash value was created. Otherwise, the data have been changed in the meantime." – D. Drescher, *The Blockchain Basics*, pp. 82–83.

18
"When the wallet is initialized or set up for the first time, an address, public key, and private key are automatically generated. Bitcoin is based on public-key encryption, meaning that you can give out the public key freely but must keep the private key to yourself." – M. Swan, *The Blockchain*, p. 3.

19
"Doing some sort of back calculation to derive the private key from the public key is either impossible (…) or prohibitively expensive (tremendous computing power operating over a longer time than would be necessary to confirm the transaction)." – Ibid., p. 99.

20
D. Drescher, *The Blockchain Basics*, pp. 99–100.

21
Ibid., p. 106.

In this way, based on the verification of all the nodes, the recipient can verify that it is indeed the specific node of the end-user that is the real sender of the message. By comparing between the hash value of data and the *cyphertext*, in case that we establish the same result, it is concluded that this is indeed the message that a user wanted to send.

1.5. Data Structure in Blockchain

Hash values and the cryptographic technology aim to provide security within the system so that the mentioned data transfer could take place. Given that a certain node owns all the data within the system, and that people can own nodes,[22] we can talk about the transfer of ownership within the system.[23]

"Actually there are no such things as intended or unintended changes in the blockchain. These words refer to a valuation of the motives or the person who caused a change. But the blockchain-data-structure values neither the motives nor the person who causes an inconsistency. The blockchain only cares about correctness and consistency of all its hash references. If one of them is invalid, the whole data structure is invalid, regardless of who or what caused that change or why it was made. And this property makes the blockchain-data-structure very valuable."[24]

However, to understand the transfer of ownership, we should first understand the *blockchain-data-structure*. The data in blockchain is structured as blocks connected by a chain (hence the name). Every block consists of two components – *header* and the *Merkle tree*.

"Each block is also hashed with the chain of previous blocks, so the entire chain of blocks is tamper-evident. This is called a Merkle tree, invented in 1979 and widely used since."[25]

All the transactional data are located in the Merkle tree, while the cryptographic hash values for every block are located in the header. Another innovation of the blockchain technology reflects in its ability to save and preserve the complete transactional data history. None of the transactions that were ever executed gets deleted, and they are available for inspection to every node at any time. Furthermore, the complete transactional data history is almost impossible to alter (immutability).[26] This characteristic represents an additional safety contribution to blockchain technology.[27] The principle of data immutability relies on the fact that any mutation of data within the blockchain is of extremely high computational cost.[28] Besides the mutation of the existing data structure in blockchain, the addition of new blocks could require[29] a lot of invested computational power, meaning an additional investment of financial resources.[30]

When we design a system of blockchain technology, only valid transactional data must enter into the data structure. To ensure that only valid transactions are going to be added to the blockchain system, all the nodes in the decentralised system of peer-to-peer computer network act like supervisors of the other nodes in the same system. Besides supervision, all the nodes reward all the other nodes in the system for adding valid and authorised transactions and for finding errors in the work of others. This mode of operation encourages all the nodes to process the data of the transactions and the transactions themselves correctly as well as to notice and denounce errors of other nodes.[31] The system of rewarding the nodes for adding valid blocks is the most important feature of an open blockchain system.[32]

Upon adding and rewarding the nodes within the blockchain system, complex mathematical operations occur, which will not be analysed in this paper. It

suffices to say that the activity of blockchain system in this particular sense can be called the blockchain algorithm.[33] The algorithm represents a group of symbols and a general process of systematically solving individual tasks belonging to a specific class of mathematical problems. Hence, the phrase "the blockchain algorithm" will be used as a simplified description of the processes that lead to the execution of the blockchain technology functions. In decentralised blockchain of peer-to-peer network of computers with a distributed ledger, there is a *competition*[34] between the nodes for adding new blocks to the system. The competition can be divided into two sections, speed competition (which node will be the fastest) and quality competition (where the focus is on the quality assessment of the validity of newly added block).

"The quality competition has an interesting aspect of peer control. By receiving a new block, each node realises that it has already lost the speed competition and that it has to work as a referee in the quality competition. It goes without saying that these referees are the most meticulous and strict referees one can imagine because they have already lost the speed competition and hence have nothing more to lose. Actually, all nodes know that they can get back in the game for

22
In this particular case meaning end-users.

23
W. Mougayar, V. Buterin, "Identity Ownerships & Representation", *The Business Blockchain* [Microsoft Edge, EPUB format]. Ownership and our identity on the blockchain are two inseparable concepts.

24
D. Drescher, *The Blockchain Basics*, pp. 132–133.

25
David Gerard, "The blockchain", para. 5., in: David Gerard, *Attack of the 50 Foot Blockchain*, Create space Independent, 2017 [Microsoft Edge, EPUB format].

26
"Immutability means that something cannot be changed. Data that are immutable cannot be changed once they have been created or written. For that reason, these data are also-called read-only data." – D. Drescher, *The Blockchain Basics*, p. 137.

27
Especially taking into consideration the fact that the decentralised system of peer-to-peer computer network is always ready to accept new nodes, hence to the blockchain we can also attribute the characteristic of transparency.

28
Ibid., p. 137.

29
Cf. ibid., p. 142. Addition of new blocks in the system could be expensive depending on the difficulty of hash puzzles: "The immutability of the blockchain-dana structure depends on the computational costs induced by the hash puzzle. The difficulty of the hash puzzles determines how much computational effort and hence how much time is needed to solve them, which in turn determines the immutability of the blockchain-datastructure." – Ibid.

30
The principle of immutability relies on finding the solution to hash puzzles. Solving hash puzzles usually demands an investment of great computer power. In every blockchain there is a difficulty level of solving the hash puzzles.

31
Ibid., p. 155.

32
"Rewarding the nodes for successful delivery of valid blocks is a basic concept of the blockchain algorithm." – Ibid., p. 157.

33
Cf. R. Wattenhofer, *The Science of the Blockchain*, Inverted Forest Publishing, 2016. Almost the entire book is imbued with the mathematical operations that lead to the solution of a certain problem. The mentioned book describes mode of blockchain operation, from the mathematical-logical perspective. Should the reader be interested in this perspective, they could commit to studying the algorithms that Wattenhofer thoroughly described in his work.

34
Competition is not strictly necessary in every blockchain system. For the particular type chosen for this paper it is logically implied. Without competition, blockchain can be used for archiving information but then there is no need for incentives for nodes in the system.

the reward if they can prove that the submitted block is invalid. In this case, the speed competition reopens and they have the chance to finish their own block, whose completion was interrupted, and to win the race themselves. As a result, the quality competition or the examination of the submitted block, respectively, will be done at a very high level of accuracy."[35]

At any moment of the competition, all the nodes of the system are found in one of two possible phases. They either a) verify a new block that is delivered by the other nodes, or b) try to be the next node that will form a new block which will be verified by the other nodes in the system.[36] The problem is how to determine unique data history in the decentralised system of peer-to-peer computer network. There is no central node that would determine which data history is the correct one, and in the decentralised architecture of computers, every node can create its data history. The question that arises is the question of *consensus*[37] that is essential for blockchain as this technology currently has the comparative advantage guaranteeing a high level of security. It is, therefore, necessary to define one chain into which all the nodes can inscribe history to maintain security. Besides security, however, if we define one chain that is agreed to be unique as it is, we will more clearly articulate what data belong to which node. If a node suggests its data history, it could try to maximise its position. By defining one chain where everyone gets as much as they contributed, the principle of *distributive justice* would be established – to each according to its merits. If it is to achieve the security of the system, then the consensus on one chain is in the interest of all the nodes in the system. Data history follows the principle of *immutability*. By adding valid blocks to the chain, the possibility that a person tries to alter data history diminishes.[38] The longer it has been since we consensually selected one and unique chain, the more blocks with valid data will be present in that chain, and the eventual consistency will be achieved.

"The deeper down the authoritative chain a block is located, the further in the past it was added, the more time has passed since its inclusion in the blockchain-data-structure, the more common effort has been spend on adding subsequent blocks, the less it is affected by random changes of the blocks that belong to the longest chain, the less likely it will be abandoned, the more accepted it is by the nodes of the system, the more anchored it is in the common history of the nodes."[39]

Precisely for the consistency that enhances as more time goes by, the system becomes resistant to manipulative changes,[40] and it becomes harder to impose some other chain as the right one.

"This is the foundation of the security of the blockchain and is the fundamental reason why a malicious node cannot propagate newly created blocks that would otherwise overwrite ('rewrite') history. Because the nonce must satisfy this requirement, and because its satisfaction depends on the contents of the block and in turn its composed transactions, creating new, valid, blocks is difficult and, over time, requires approximately the total compute power of the trustworthy portion of the mining peers."[41]

We can conclude that the decentralised system of peer-to-peer computer network guarantees more security to the users than any other technology before. This additionally intensifies the argumentation towards its usefulness. For a blockchain system to be secure, nodes are delivering *proof of work*. The question is – why are they motivated to do so?

To motivate nodes to continue delivering *proof of work*, there has to be some model of reward. It is difficult for the blockchain system to be sustainable without it.[42]

If we want to use blockchain technology exclusively for data storage, then we do not find any problem with the reward system. Moreover, we do not need

it. But blockchain technology has been recognised as a great foundation in new projects aimed at creating electronic money. Systematic rewarding and solving problems with the node payment instrument fit perfectly into such projects. By paying electronic money to nodes, they are also motivated to contribute to the maintenance of the blockchain system in the background as a technological solution that provides security based on its components.

For this reason, project *Bitcoin* was launched, the project of the first cryptocurrency. In the system of cryptocurrencies nodes benefit from all the privileges of the blockchain technology while, by continual delivery of evidence of work (*mining*), they are rewarded mostly by receiving *cryptocurrency* of that system they belong to. Cryptocurrencies achieve certain value that can be determined at the stock exchange.[43] We can ascertain that the value is extremely volatile, that is it oscillates from day to day, even from hour to hour.[44] For most of the cryptocurrencies, the transactional data are inscribed to a distributed ledger that is available to everyone. The concept of a distributed ledger was also mentioned in the arbitrary definition at the beginning of this paper. The distributed ledger keeps the transactional data, mirroring the *blockchain-data-structure* while, along the lines of blockchain algorithm, it uses the consensus of the majority of nodes to choose a chain that authentically describes the ownership of nodes and the executed mutual transactions.

35
D. Drescher, *The Blockchain Basics*, p. 158.

36
Cf. "Developer Guide", *Bitcoin*. Available at: https://bitcoin.org/en/developer-guide (accessed on 26 August 2020). Cf. R. Herian, *Regulating Blockchain*, p. 18.

37
Ibid., p. 18.

38
It is about the case of so-called *51% atack* that represents one of the weakest points of the blockchain technology that can easily become the corruptive elemet and where the use of technology could serve to morally questionable intents of certain individuals or interest groups.

39
D. Drescher, *The Blockchain Basics*, p. 177.

40
Cf. Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", *Bitcoin Project*. Available at: https://bitcoin.org/bitcoin.pdf (accessed on 16 August 2020).

41
Gavin Wood, "Ethereum: A secure decentralized generalized transaction ledger", *Gavin Wood* (2014), p. 7. Available at: http://gavwood.com/paper.pdf (accessed on 15 August 2020).

42
D. Drescher, *The Blockchain Basics*, p. 179.

43
Official website of the stock exchange, available at: https://coinmarketcap.com/ (accessed on 20 August 2020).

44
Market capitalisation on 20 September 2020 at 12:01:00 (UTC + 01:00) amounted to 351,791,488,569 (three hundred fifty-one billion, seven hundred ninety-one million, four hundred eighty-eight thousand, five hundred sixty-nine) American dollars, while the volume of stock-exchange in 24 hours at the same time (total value of all transactions) amounts to 99,244,850,090 (ninety-nine billion, two hundred forty-four million, eight hundred fifty thousand, ninety hundred) American dollars. At the beginning of 2020, on 7 January at 12:02:00 (UTC + 01:00) to be precise, market capitalisation was 211,009,239,809 (two hundred eleven billion, nine million, two hundred thirty-nine thousand, eight hundred nine) and the volume was 83,188,036,236 (eighty-three billion, one hundred eighty-eight million, thirty-six thousand, two hundred thirty-six) American dollars. Available at: https://coinmarketcap.com/charts/ (accessed on 26 December 2020).

1.6. What Distinguishes Blockchain from Other Technologies

Conceptual and architectonical design of the *blockchain* technology lies on seven principles.[45]

1) Networked integrity: the first principle is values of integrity and trust within the system that blockchain aims to achieve. A. Tapscott and D. Tapscott will say that these values are inscribed into the blockchain code, but that does not mean that people are amnestied from them. On the contrary, if we look at technology as a product of human labour and intellectual achievement whose goal is to facilitate and simplify specific tasks, then we can acknowledge that the referential point of technology implies a human being.
2) Distributed power: the second principle is the distribution of power within a network. The absence of a central entity enables everyone to contribute to the system and supervise the other nodes. Distribution of power is mentioned by some researchers when arguing the topic of digital democracy.[46]
3) Value as an incentive: working on inherently inscribed values in the technology of blockchain is motivational for all the nodes and encourages them to contribute to the system as much as possible because of the system of rewards. It is best manifested in the best-known implementation of the blockchain – cryptocurrencies.
4) Security: security is another innovative element offered by blockchain. Security is to be achieved through the contribution of all the nodes to the values that their creators had inscribed into the blockchain. Two components which form blockchain, cryptography and hash values, facilitate the mentioned.
5) Privacy: although debatable for some, even for A. Tapscott and D. Tapscott, in the field of blockchain, privacy is innovative as it tries to be accomplished in the decentralised system with a presupposed minimum of trust towards all the other nodes. There is a certain tension point between the privacy and transparency in the blockchain. Namely, how to maintain a right to privacy of every node in the decentralised system with a distributed ledger, while making it open for everyone.
6) Rights preservation: the concept that represents a difference and one of the main characteristics of blockchain is the so-called *smart contract*.[47] The smart contract enables the transfer of ownership from one node to the other, where the system itself, that is the other nodes, can verify whether both parties respect contractual agreements or not and, in case of a dispute, can act as mediators.[48] This is the ultimate implication of the mediation abolishment in the domain of blockchain.
7) Inclusion: we could ask ourselves how much is the blockchain technology inclusive? Jared Norton states that what makes the blockchain technology different is that it can be inclusive for everyone.[49] As a cause, he identifies the fact that there are no rules (at least for now) according to which someone would be allowed into the world of blockhain, no entrance fees (except the minimum that requires you to own some mobile device by which you could connect to the Internet) and "friendly environment" due to the principle of anonymity. If I would like to provide a service to a particular person, I could do so with minimal risk, that is

> with great trust in people whose name and surname I am not required to know.[50]

The most important feature of the *blockchain* technology is this: it aims to build and maintain *integrity* and *trust* within the decentralised system of peer-to-peer computer network with a distributed ledger (where we cannot estimate the level of trust in the other nodes) through the cryptographic and hash technology. Exclusively in this system, the transactional data being exchanged between all the nodes are available on the distributed ledger and are visible in every moment. Although from the technical point of view, this is ensured by the technological components, there still exists the non-technical factor. Modern-day computers are still probabilistic and have developed neither consciousness nor self-consciousness and cannot decide without programming. Human beings program software and design machines, which makes them the representatives of the non-technical aspect. The *blockchain* is built from the people for the people, like any other technology, and can be considered successful if it has integrated into society.

2. Ethical Foundations of Blockchain Technology – Ethical Aspect

Martin Peterson argues that it is crucial to separate normative and applied ethics, as normative ethics aims to find the causal justification, while applied ethics relates to specific situations in real events.[51] However, Peterson continues to develop his theory and claims that ethical theories cannot deliver the final moral judgement in the questions of applied ethics. With applied ethics, we cannot know if there even exists any correct ethical theory. According to Peterson, in the world of technology, there are five specific principles that help us make a decision in a given case when there is a moral dilemma: cost-benefit principle, the principle of caution, the principle of sustainability, the principle of autonomy and principle of fairness.[52]

If we want to find the answer to the question of whether it is justified to conduct a 51% attack[53] in the *blockchain* system, we should run it through five

45
Cf. A. Tapscott, D. Tapscott, "The seven design principles of the the blockchain economy", in: A. Tapscott, D. Tapscot, *The Blockchain Revolution* [Microsoft Edge, EPUB format].

46
Carl Miller, "TEDx Talks: Digital Democracy", *TedxTalks*, *YouTube* (4 May 2016). Available at: https://www.youtube.com/watch?v=FNL22RvFwn0 (accessed on 11 September 2020).

47
"… smart contracts are certainly not capable of supplanting contract law as we presently find it, but the hope of many stakeholders is that they soon will." – Robert Herian, *Regulating Blockchain Law*, p. 39.

48
Cf. M. Swan, *Blockchain*, p. 16.

49
Jared Norton, *Blockchain: Easiest Ultimate Guide To Understand Blockchain*, Create Space Independent Publishing Platform, 2016, p 19.

50
Ibid., p. 20.

51
Martin Peterson, *The Ethics of Technology. A Geometric Analysis of Five Moral Principles*, Oxford University Press, New York 2017, p. 5.

52
Ibid., p. 14.

53
I shall further discuss the problematic of 51% attack in a separate part of this paper.

mentioned principles. However, this still tells us nothing about the non-technical aspect:

"Each principle states a necessary condition for a technological intervention to be morally right, but no individual principle is sufficient for determining the rightness of an intervention on its own. The rightness of some technological interventions depends on several principles."[54]

At the moment, we are not interested in the moral implication of the use of *blockchain* as a technology behind, for example, a digital voting system. We are interested in values that are implemented into the core of technology and write primarily about the rightfulness of the usage, as can be concluded from the quote. Furthermore, a description of the potential attackers would fall within the domain of descriptive ethics. Since the development of the *blockchain* technology is still ongoing, we have too little information according to which we could make a description on which we could build the potentially applied ethics for the blockchain. We are now in the domain of applied ethics, and we entered into one part of it – ethics of technology. In this field, Luciano Floridi devised two very interesting terms that will help us put the problem into context. He talks about *infosphere* and *re-ontologising*.[55]

Infosphere is a term formed following the model of *biosphere*. It comprises the entire informational environment that consists of informational entities and their features, interactions, processes they perform and mutual connection. Floridi states that this is the concept that rapidly evolves. For this reason, in the informational environment that consists of all the informational entities, reengineering occurs that not only affects the technical aspects of the system but fundamentally changes the intrinsic nature, that is the ontology or the essence of that system. One of the best examples of re-ontologising of the infosphere is the transition from analogue to digital data. One of the main issues Floridi underlines is the ontological friction, where the information is not distributed within the system. He sees the solution in making humanity aware of the fact that it is the most liable one in the age of rapid growth of informational-telecommunications technology, and thus he offers a suggestion in the form of e-nvironmental ethics[56] that mediates nature (*physis*) and technology (*techne*).[57] That coexistence is crucial as the infosphere itself represents the communal space that should be preserved for the benefit of all people. Why is Floridi important in this argumentation, one might ask. Precisely because the technical aspect of that technology enables incorporated values found in the core of the blockchain (*integrity* and *trust*).[58] The technical standard set to maintain those values is really high, and the evolution of the entire depends on it, also forcing people to respect them. It seems that the blockchain system in its core represents an attempt to abolish ontological friction which is a precondition for e-nvironmental ethics where nature and nurture strive to be reconciled.[59]

Elaboration of the matter moves towards the article of Philip Brey, who examines values in technology.[60] This article is important as it deals with the values that I detected in the very core of blockchain technology (*integrity* and *trust*). Brey talks about *built-in-consequences*[61] that are not absolute but depend on the context of usage of a certain technology. The *embedded value* is a special kind of embedded consequence.[62] When addressing the values, technological entities can either encourage or harm the realisation of certain values. When this activity, whether harmful or useful, takes place systematically in all technological entities in a system, then we talk about the tendency to promote certain value. This built-in tendency is called *embedded value*. Since they

are present in all entities, these values, as they are, shape the system because they often focus on the moral norms. The norms are usually based on values; they use them as a stronghold and reference point. If there is a promotion of certain embedded values in the system, then we can conclude that this norm is embedded in the system (*embedded norms*).[63] Embedded values can be intentional.[64] This is important especially for decentralised systems, such as blockchain. We can state that in the blockchain system, there exists an intention with embedded values of integrity and trust that aim to maintain security. Hence, we can conclude that the *blockchain*, from the technical point of view, fundamentally aims to promote useful values. Brey argues that the most important feature of disclosive computer ethics lies in the possibility that the moral features will not remain opaque and become more transparent, which will in return enable ethical analysis and moral decision making.[65] The efficiency of such an ethical approach is increased in decentralised systems of peer-to-peer computer network because of embedded values. Brey argues that the design of informational systems, in general, became sensible and more aware of the values that are intended to be intentionally incorporated into the system. This way, we encounter the term *value-sensitive design*:

54
M. Peterson, *The Ethics of Technology*, p. 14.

55
Luciano Floridi, "Ethics after the Information Revolution", in: Luciano Floridi (ed.), *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press, New York 2010, pp. 3–19, p. 6.

56
Ibid., p. 17. When Floridi, in a wordplay, separates the term *e-nvironment*, by the first letter "e" refers to the term *ekopoiesis*.

57
L. Floridi, "Ethics after the Information Revolution", pp. 18–19.

58
Cf. subchapters 1.3. and 1.4. of this paper.

59
The point of reconciliation enters the domain of ontology. A person, being prosthetic (related to technique), is inherently also self-destructive. Being of a person is in constant danger from its own activity. Technology is at the same time an inexhaustible source of the possibility of progress and the abyss of a person's own destruction. Cf. Bernard Stiegler, *Technics and Time, 1: The Fault of Epimetheus*, translated by Richard Beardsworth, George Collins, Stanford University Press, Stanford 1998, p. 196.

60
Philip Brey, "Values in technology and disclosive computer ethics", in: L. Floridi (ed.), *The Cambridge Handbook of Information and Computer Ethics*, pp. 41–58, p. 41.

61
Ibid., p. 45.

62
Ibid., p. 46.

63
Ibid., p. 47.

64
Ibid., p. 50.

65
"The importance of disclosive computer ethics is that it makes transparent moral features of practices and technologies that would otherwise remain hidden, thus making them available for ethical analysis and moral decisionmaking. In this way, it supplements mainstream computer ethics, which runs the risk of limiting itself to the more obvious ethical dilemmas in computing. An additional benefit is that it can point to novel solutions to moral dilemmas in mainstream computer ethics. Mainstream approaches tend to seek solutions for moral dilemmas through norms and policies that regulate usage. But some of these moral dilemmas can also be solved by redesigning, replacing or removing the technology that is used, or by modifying problematic background practices that condition usage. Disclosive ethics can bring these options into view. It thus reveals a broader arena for moral action, in which different parties responsible for the design, adoption, use and regulation of computer technology share responsibility for the moral consequences of using it, and in which the technology itself is made part of the equation." – Ibid., p. 53.

"In ethics (VSD) represents an interesting shift of focus from human actions to technological artefacts and systems. In computer science, (VSD) represents an interesting shift from utilitarian and economic interests to care for human values in design. As a result, (VSD) promises new and more complete computer ethics as well as enhanced design practice in computer science and engineering, what could result in a technology that follows our moral and public values."[66]

Briefly, VSD is significant because it does not care only for values in the operating system but also that those values follow our moral and public values. In VSD, there is the tendency to incorporate only the best possible values in our system. In other words, VSD tends to promote the best possible values that reflect public values, namely *virtues*.[67] Hence, this is the first sign that it would be most appropriate for our further research to set forth in the direction of virtue ethics.[68]

To better understand why it is that virtue ethics is the most compatible with blockchain technology, I will also briefly mention consequentialist and deontological ethics. Consequentialist ethics puts the focus on the consequences. In short, everything that maximises good consequences is morally justified.[69] Thus, utilitarianism would be a part of consequentialist ethics.[70] According to Graham, utilitarian ethics has two important aspects: hedonistic (relating to pleasure and happiness) and consequential (relating to consequences of action).[71] I omit the hedonistic aspect and will mention that the consequentialistic aspect in its two important momenta includes the intention of the one that acts and the chain of responsibility that such an action implies. The consequences are important from the moral aspect,[72] however, what is "good" still remains vague. John Stuart Mill attempted to answer this question through the evidence of the utilitarian principle.[73] When I examine his evidence and try to place it within the subject of the paper contextually, I conclude that Mill's law relates to what we have resolved from the technical aspect. The blockchain technics, based on its two components, represent a useful basis to many different projects in the ongoing applications of blockchain. In this case, the technical use of this technology, based on technical-performance solutions, is an extension of blockchain that goes from the core with the inbuilt values of integrity and trust. Mill puts his focus on usefulness:

"It is proper to state that I forego any advantage which could be derived to my argument from the idea of abstract right, as a thing independent of utility. I regard utility as the ultimate appeal on all ethical questions; but it must be utility in the largest sense, grounded on the permanent interests of a man as a progressive being."[74]

Unlike Mill, Kant would instruct us to do good because that is our duty.[75] Within work of Kant one can find there are categorical imperatives that construct the rules of moral behaviour.[76] Most explicitly, the idea is elucidated by the formulation of his fundamental imperative, to "[a]ct in such a way that the maxim of your will can always simultaneously hold as a principle of a universal legislation".[77]

Kant also discusses the good[78] and the importance of intention[79] in achieving the good. Kant would state that moral conceptions are *a priori*.[80] Although Kant writes about moral conceptions, he builds his research on the idea of freedom that is a precondition of will from which good or bad actions are subsequently derived, according to the conscience of every individual that conforms to the maxim of the golden rule.[81] *I want* is overpowered by what *must* be done, and with Kant categorical imperative takes primacy.[82] Blockchain technology seeks to achieve integrity and trust in the system with its values embedded in the system. To incorporate these values from a non-technical

point of view, it is extremely important to start a discussion about values, especially virtues, and explain why they can positively affect the blockchain system.

In non-technical domain virtue can be characterised as a good habit[83] or an excellent feature of character.[84] From general sources on virtue ethics we can learn that this discipline has always emphasised the importance of education on morals (beginning with Plato's *Politeia* and Aristotle's *Nicomachean Eth-*

66
Ibid., p. 42.

67
Cf. Batya Friedman *et al*., "Value Sensitive Design and Information System", in: Kenneth Einar Himma, Herman T. Tavani (ed.), *The Handbook of Information and Computer Ethics*, John Wiley & Sons Inc., New Jersey 2008, pp. 69–101, p. 70.

68
Ibid., pp. 87–89. Authors suggest to perform a conceptual investigation of key values which can be read about in next chapters and subchapters of this paper. The reason why the analysis has been shifted to the virtue ethics is because of the specific technical part of the blockchain, namely its two main components. Authors also suggest that based on technological design "a given technology is more suitable for certain activities and more readily supports certain values while rendering other activities and values more difficult to realize". – Ibid., p. 73. Based on this, I concluded that the best match for blockchain technology is virtue ethics.

69
Harry J. Gensler, *Ethics. A Contemporary Introduction*, Routledge, New York 2011, p. 110.

70
"Utilitarianism understands that all actions must be judged exclusively through the consequences they have on luck (…)." – Gordon Graham, *Theories of Ethics. An Introduction to Moral Philosophy with a Selection of Classic Readings*, Routledge, New York 2010, p. 103.

71
Ibid., p. 103.

72
Ibid.

73
John Stuart Mill, *Utilitarianism*, Oxford University Press, New York 1998, p. 88. Cf. G. Graham, *Theories of Ethics*, p. 114.

74
John Stuart Mill, *On Liberty*, Batoche Books, Kitchener 2001, p. 14.

75
Immanuel Kant, *The Critique of Practical Reason*, translated by Philip McPherson Rudisill, *Kant and Wesley* (12 September 2012), p. 128. Available at: https://kantwesley.com/Kant/CritiqueOfPracticalReason.pdf (accessed on 23 January 2020).

76
Ibid., p. 19.

77
Ibid., p. 38.

78
Immanuel Kant, *Foundations of the Metaphysics of Morals*, translated by Lewis White Beck, Bobbs-Merrill Educational Publishing, Indianapolis 1959, p. 9. Cf. G. Graham, *Theories of Ethics*, p. 79.

79
G. Graham, Theories of Ethics, p. 80. Cf. "With this capacity transcendental freedom will also stand firm and indeed in that absolute sense which speculative reason required with the usage of the concept of causality in order to save itself from the antinomy into which it unavoidably stumbles if it contemplates the unconditioned in the series of causal connection. But it could only set up this concept problematically as not impossible to think, without securing its objective reality, but rather only not to be assailed in its existence nor be toppled into an abyss of skepticism through the vain impossibility of that which it must still allow as at least thinkable." – I. Kant, *The Critique of Practical Reason*, p. 1.

80
In this case, *a priori* does not mean temporal, but logical – it represents the generality and necessity of validity independent of experience. Kant does not intend to establish the new principle of morality. By the analysis of moral consciousness, he comes to the concept of good will. It is the only entity in the world that is good in itself and without limitations. It carries its purpose inside itself, which is the fulfilment of duties. Duty is a necessity of acting from respect for the law within us. For Kant, the concept of good and evil does not have to be determined before the moral law (operated by duty), but only after it and through it. The maxim of action is ahead of

→

ics) not as the application of certain rules, but the training of our character.[85] Furthermore, general sources state that, although the research in scope of virtue ethics significantly evolved in the last 35 years, it is still not so actual, especially in the field of applied ethics.[86] However, what separates virtue ethics form consequentialism and deontological ethics is that it puts virtues as features of character in focus of its research.

Despite the time passed, Plato and Aristotle are particularly significant for virtue ethics and the *blockchain* phenomenon. In *Politeia*, Plato mentions that only the philosophers-emperors can make a state prosperous.[87] Everyone in the State prosper when we distribute the working roles and Plato believes that there are three classes in every state: commercial, auxiliary and decision – making.[88] Therefore, distribution of the roles in a state attains justice. Plato argues that the soul has rational, spirited and desiring part.[89] To achieve harmony between the three parts of the soul also means justice, but in this particular case – justice of an individual. Justice of an individual does not differ from a State's justice as there is a common idea of perfect justice.[90] It is important to mention that Plato finds that all the attention in a State has to be focused on nurture and education.[91] Plato would ascertain that no one is evil by their choice but are made evil by, *inter alia*, inadequate education.[92] In his philosophy, the highest idea is the idea of the Good, and everything strives towards it.[93] The material world is derived from the ideas so the ideas represent genuine reality and objectivity. Although the world of ideas is transcendental for the human, that does not mean that he should not persist in his observance.[94] This is also an important moment. If we isolate Plato's doctrine from the context and try to apply it to the non-technical aspect of the *blockchain* technology, we should pay our attention to the philosophy of education and the perseverance in our aspiration to become better people. In this way, we can construct a system that is beneficial for everyone.

Aristotle greatly expanded and elaborated Plato's doctrine. Aristotle believes that a person is good when they act in a manner of thoughtfulness, and this kind of practice implies the righteous mind.[95] The righteous mind acts when our deeds are beautiful, and in order for them to be beautiful, we should adhere to the so-called golden middle between what is too much and too little (for example, according to Aristotle, courage is the middle between fearfulness and complete boldness).[96] Consequently, virtue is situated in precisely this golden means. According to Aristotle, if we act upon virtue, we will gain bliss (*eudaimonia*).[97] Virtue is a way of conduct by which a person acts well, but consequently also becomes good. Every person should seek the middle regarding themselves, and what represents a reasonable middle for one person, does not have to apply to the other.[98] However, as Aristotle emphasised, what an individual considers to be good for them in a certain moment can differ from what truly is good.[99] Achieving the genuine Good should be our ultimate objective, and by its achievement, a person becomes virtuous. As this path is difficult, Aristotle, for this reason, emphasised possessing the practical wisdom and the capacity for judgement as being the features of a moral human being.[100] It should be pointed out that Aristotle divided virtues into moral virtues and intellectual virtues.[101] While moral virtues refer to emotions, intention and action, dianoetic virtues refer to seeking the truth, that is, pure knowledge.

Unlike Kant,[102] Aristotle does not offer the rules to follow. It is about the responsibility for acting upon one's own judgement since a person has the

power to build themselves and aim to bliss, that is to say, it is on a person to determine what is good for them in a certain moment while striving for their individual goods to align with the genuine good. For this kind of reasonable acting, a person undoubtedly has to possess knowledge and experience.[103] Aristotle is the one who points us in the direction we could follow when we discuss our subject – investing in our knowledge and gaining experience will facilitate the making of reasonable decisions that will have a virtuous effect not only on us but the people around us. Aristotle criticised Plato's doctrine on the ideas that divide the world of ideas from the material, sensory world. Aristotle believed that weakness lies in the fact that Plato puts the essence into ideas and then positions them into the transcendence. The essence, however, cannot exist separately from what it is in, as holds Aristotle.[104] From the technical aspect, the *blockchain* will assure the security within the system, but it

the theoretical cognition of good and evil. Cf. I. Kant, *The Critique of Practical Reason*, pp. 100–118.

81
"Indeed the moral law is given as a factor, as it were, of pure reason. We are conscious of it a priori and its certainty is apodictic, even though we may be unable to ferret out in experience a single example of perfect compliance with it." – Ibid., p. 62.

82
Ibid., p. 53.

83
H. J. Gensler, *Ethics*, p. 139.

84
Rosalind Hursthouse, Glen Pettigrove, "Virtue Ethics", *The Stanford Encyclopedia of Philosophy*. Available at: https://plato.stanford.edu/archives/win2016/entries/ethics-virtue/ (accessed on 25 August 2020).

85
Plato, *The Republic*, translated by Tom Griffith, Cambridge University Press, Cambridge 2000, 403d–403e.

86
R. Hursthouse, G. Pettigrove, "Virtue Ethics".

87
Plato, *The Republic*, 485.

88
Ibid., 441.

89
Ibid., 439e–442c.

90
Ibid., 441c–441d.

91
Ibid., 416b–416d.

92
Ibid., 419–421c.

93
Ibid., 608e–609b.

94
Ibid., 621c–621d.

95
Aristotle, *Nicomachean Ethics*, translated by Roger Crisp, Cambridge University Press, Cambridge 2004, 1095b.

96
Ibid., 1104a.

97
Ibid., 1098b.

98
Ibid., 1095a.

99
Ibid., 1094b.

100
Ibid., 1179a.

101
Ibid., 1103a.

102
Immanuel Kant, "Transition from popular moral philosophy", para. 46, in: *Fundamental Principles of the Metaphysic of Morals*, translated by Thomas Kingsmill Abbott, Project Gutenberg, 2004 [Microsoft Edge, EPUB format]. In his *Metaphysics of Morals*, Kant rigorously analysed the rules for duties with which one fulfills the maxims that can subsequently be generalised. In the quote I mentioned, the third of existing four that appear in the book, Kant primarily refered to the act itself while Aristotle argued about character of a person.

103
Aristotle, *Nicomachean Ethics*, 1142a.

104
Aristotle, *Metaphysics*, translated by Hugh Lawson-Tancred, Penguin Group, London 1998, 1077b [Freda, EPUB format].

leaves a small margin of discretion that opens great possibilities to a person – how will this technology be used and will that be for general welfare or the welfare of certain individuals and how to coordinate technics and people with virtue?

Physis and *techne* have never been closer than in the *blockchain* technology, that is, technical and non-technical side of technology have never been so connected.[105] If, on the one hand, there are values of trust and integrity that aim to achieve security based on innovative technology, analogously, on the other hand, we should seek the values that an individual should possess in order to complete those values, but also to make one step further. For that to happen, we need a person of virtue, that is, we need more people of virtue.[106] To obtain virtues, one should continuously work on themselves and invest in their knowledge and experience. Only by raising and standardising the system of values can blockchain come to life in the way it is supposed to – to humankind's benefit.[107] Albeit the critics would say this is not possible, we can refer them to the platonic approach – to continually improve our knowledge[108] and enlighten people. Only in this way will the education of younger generations truly gain ground, by standardising and awarding positive system of values. The principle (in Greek) of *gnothi seauton* still applies because we can make blockchain technology to maintain its integrity and gain consistency over time.

3. Determining Moral Challenges of Blockchain Technology[109]

3.1. Positive Application of Blockchain Technology

I indicate several positive examples of the application of blockchain technology and several possibilities of its future use.[110]

I already mentioned *cryptocurrencies* – they have the potential to manage the ownership, and they create an innovative model of payment that can be independent of the central entities, such as banks or governments. Micropayments are another use. This involves paying extremely small amounts of money that are not cost-effective to claim and pay through banks as intermediary institutions, as it is currently done. The technology could be used as a form of safe storage of identity of natural persons that functions on the principle of cryptography. All personal documents could be deposited in the *blockchain*, which would eliminate the need for issuing these documents in physical form (for example identity card, driver's license, health insurance card, etc.). Furthermore, there could be deposited different documents, legal files, contracts digitalised before the deposition, etc.). Another interesting possibility arises in the field of taxation. Calculation and collecting the tax could be done through the list of owners in the blockchain system, eliminating double taxation (modelled on *double-spending*) or tax evasion.[111]

Voting could also be carried by blockchain technology, from creating the ballots to their distribution throughout the system and collecting the votes. Blockchain can serve as a background technology for many projects involving digital money. Besides, projects of this kind have already been launched.[112] A. Tapscott and D. Tapscott hold that by transposing the paradigm of voting to blockchain, one will ensure fair, safe and easy voting[113] and indirectly tackle

the problem of passive citizens. A. Tapscott and D. Tapscott also state that the possibilities the *blockchain* offers in this segment do not stop on voting:

"Everyone has a right to take part in the government, directly or by voting. Whoever is elected must conduct affairs in the full light of day as a peer among peers. With the Internet, citizens took more responsibility for their communities, learned from and influenced elected officials and vice versa. With blockchain, citizens can go one step further: they can advocate for sealing government action in the public record in an unalterable and incorruptible ledger. Not just checks and balances among the powerful few but broad consensus of the many, for example, to effect background checks on potential gun owners."[114]

If this sounds like an implausible scenario, it should be mentioned that in Estonia[115] and Ukraine,[116] there are projects[117] launched in both public and private sector based on blockchain technology.[118]

105
M. Heidegger, *The Question Concerning Technology and Other Essays*, translated by William Lovitt, Garland Publishing Inc., Harper and Row, New York 1977, pp. 32–33.

106
"To put the same point more contentiously, from a virtue ethicist's perspective, utilitarian thinking is merely 'logistical' (i.e. cunning) and, as such, resembles the thinking of evil men (…). In other words, truly good and noble behavior requires looking at one's motives for thinking some argument is compelling, not merely in simply lining up reasons pro and con for a particular course of action (…)." – Daryl Koehn, "A Role for Virtue Ethics in the Analysis of Business Practice", *Business Ethics Quarterly* 5 (1995) 3, pp. 533–539, p. 535, doi: https://doi.org/10.2307/3857397.

107
"Taking virtue ethics seriously will probably mean that one ultimately has to choose one system over the other." – Ibid., p. 536. Koehn does not argue that utilitarian ethics is bad or that virtue ethics is aboslutely right in every aspect. He stresses that one has to choose which system he will use in the real-life business situations.

108
Plato, *The Republic*, 514–517.

109
Moral challenges presented in this paper arise mainly from the technical aspect of blockchain. The proposed solutions, or how to overcome them, are done through Heidegger's and Stiegler's view on technology in general. However, moral challenges regarding blockchain technology will hopefully be researched more in the future.

110
Cf. R. Jesse McWaters, "The future of financial services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed; an Industry Project of the Financial Services Community", *World Economic Forum 2015*. Available at: http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf (accessed on 23 August 2020).

111
Cf. D. Drescher, *Blockchain Basics*, p. 227.

112
M. Swan, *Blockchain*, p. 49.

113
A. Tapscott, D. Tapscott, "The second era of democracy", para. 1, in: A. Tapscott, D. Tapscott, *Blockchain Revolution* [Microsoft Edge, EPUB format].

114
A. Tapscott, D. Tapscott, "Something is rotten in the state", para. 12, in: A. Tapscott, D. Tapscott, *Blockchain Revolution* [Microsoft Edge, EPUB format].

115
Avaliable at: https://e-estonia.com/tag/blockchain/ (accessed on 29 October 2020).

116
Available at: https://bau.ai/en/ukraine-en/ (accessed on 29 October 2020).

117
Notable mention for public blockchain projects goes to the United Kingdom and Ghana, Kenya and Nigeria. Cf. Philip Boucher, Susana Nascimento, Mihalis Kritikos, *How blockchain technology could change our lives*, STOA, Brussels 2017, p.18.

118
W. Mougayar, V. Buterin, "Governments and Governance", para. 4–5, in: W. Mougayar, V. Buterin, *The Business Blockchain* [Microsoft Edge, EPUB format].

Furthermore, reputation is significant in the business world,[119] and blockchain technology can greatly impact it. For example, as a kind of auxiliary technology, it can be used with *smart contracts* whereby it is visible how many times certain natural or legal person did not adhere to its obligations arising from the contract, what could finally be resolved by the refund for the affected party.[120] This is one of the examples of successful functioning of blockchain technology due to its transparency.[121] More on point, Drescher expresses his opinion that blockchain technology will undoubtedly enable more people around the world to participate in the global market.[122]

3.2. Technical Limitations of Blockchain Technology

Jared Norton states that, although innovative, blockchain technology is still probabilistic. In other words, it can serve well when it comes to ensuring security and data storage, but, to an individual, it cannot provide answers to the questions like: "Should I evict my tenants if they don't pay the bills for six months in a row?". It is to be concluded that we cannot entirely rely on this technology.[123] In the blockchain system, if there is a cryptocurrency in the background, it implies public ledger. All the transactions are public and available to everyone. In addition, we already know that new nodes can be included in the system, continously. In this way, blockchain technology aims to achieve transparency. However, although transparent, in this case, one could raise the objection of insufficient privacy. What is more, this is the constitutive element of this technology – the dilemma lies between transparency and privacy, and so the question arises regarding how blockhcain technology can be available to everyone while maintaining the privacy of an individual?

The next objection can come from the security aspect. The only thing connecting the real owner with their ownership in blockchain system is the private key. The private key is an absolute necessity if one wants to have access to their ownership. Should it be lost either by accident or by some misfortunate event, the real owner cannot access their property. There is no other way for the owner to get hold of what belongs to them.

Furthermore, to include one or more nodes into the decentralised system based on blockchain technology, it is necessary to invest certain funds to purchase computer parts. Computers use a lot of energy to solve hash puzzles, which results in a significant consumption of electrical energy. This means that funds have to be invested in order for the decentralised blockchain system even to initiate. This brings us to the next problem – if the costs are high, not everyone can invest in this process. From the very beginning, people without the initial capital are prevented from entering into the market competition and being the blockchain participants (in the sense of an individual node in the system). Thus emerges the scenario in which one person, or a small group of people, cooperatively control most of the nodes in the system. There emerges a disguised central entity that is unknown to the other nodes in the system. The presumption coming with the blockchain system is that the nodes are of good intentions or will at least become such. One way to withstand the attack of an interest group or an individual is the growth of the technology itself to the point where this attack will be almost impossible to execute.[124] However, there will be no attack if reasonable people prevail in society. The reason is an "ethical organ" of knowledge, the power of contemplation of the things that are advantageous for a good life, the ability of action towards reason with regards to both good and bad things; it is indeed in itself the "well-doing"

(*εὐπραξία*).[125] The virtue of reason and all the other virtues, do not represent mere ancient inscriptions that are a subject of dreary studies. On the contrary, in this case, we are reaching those virtues by a detour, through technology:

"Rather, precisely the essence of technology must harbor in itself the growth of the saving power."[126]

Heidegger developed his idea by writing that from technology, besides the saving power, it appears dangerous.[127] However, this does not represent the alert or the stop sign. Heidegger then explains:

"In what respect does the saving power grow there also where the danger is? Where something grows, there it takes root, from thence it thrives. Both happen concealedly and quietly and in their own time."[128]

Because, for Heidegger, "the question concerning technology is the question concerning the constellation in which revealing and concealing, in which the coming to presence of truth, comes to pass".[129] By deduction we can conclude: if we agree with Heidegger, then this applies to any technology, including blockchain technology. Values incorporated in blockchain could shine in all their glory, as virtues, provided that people managing the technology act upon virtue and are trying to be good:

"Practical wisdom is not the same as this capacity, though it does involve it. And, as we have said and as is clear, virtue is involved in this eye of the soul's reaching its developed state. For practical syllogisms have a first principle: `Since such-and-such is the end or chief good', whatever it is (let it be anything you like for the sake of argument). And this is evident to the good person alone, since wickedness distorts our vision and thoroughly deceives us about the first principles of actions. Manifestly, then, one cannot be practically wise without being good."[130]

Another objection regarding the technical aspect of the *blockchain* technology is the inability to upgrade the existing technology (meaning primarily the component of cryptography) or to change, that is to replace the technical components.[131] That would suggest that the technologies that constitute the bases of the *blockchain* have to endure as long as the *blockchain* itself, and this duration cannot be exactly predicted – it can last for centuries. Namely,

119
J. Norton, *Blockchain*, p. 16.

120
Ibid., p. 16.

121
"So if it requires a reliable and transparent way to keep records, the blockchain can be used as a base to build an app for that." – Ibid., p. 17.

122
Ibid., p. 27.

123
J. Norton, *Blockchain*, p. 22.

124
This refers to the strengthening in blockchain (*eventual consistency*).

125
Aristotle, *Nicomachean Ethics*, 1140b.

126
M. Heidegger, *The Question Concerning Technology and Other Essays*, p. 28.

127
Ibid., p. 28.

128
Ibid.

129
Ibid., p. 33.

130
Aristotle, *Nicomachean Ethics*, 1144a.

131
Hash values and cryptography are accepted as the two components that can be conceptually altered.

making alterations or fixing errors in the system of *blockchain* technology is difficult, and that characteristic makes this technology extremely inflexible.[132]

3.3. Non-technical Limitations of Blockchain Technology

When speaking of non-technical limitations, I emphasise the two aspects: legal limitations and limitations of use. We have seen that the *blockchain* technology interferes with the concept of ownership. One of its first, necessary and most interesting applications is in the field of *cryptocurrencies*. In order for the technology to continue evolving, the legislature and the administrative settings of the countries, if they are to use the benefits offered by this technology, will without any doubt have to start considering the implementation of the legislative framework that would define the management of ownership not only in the domain of cryptocurrencies but possibly in blockchain technology in general.[133] Even if we, to a certain level, resolve the confusion created by the inexistence of legislative frameworks, there still remains a concern, or better to say a risk, what kind of ground will this technology gain. If people show no interest in this technology, it will not exist. If there will be no nodes that resolve complex mathematical problems and create new blocks, every further effort becomes futile.

Thus far, I cannot state that blockchain is more "moral" than some other technology. This technology is conceptually and theoretically well conceptualised. However, this is no guarantee that it will become absolutely the best technology, whether concerning the issues it is based on, or from the technical-conceptual side. I have to admit, there are two sides to the narrative, but regardless of the risks, regardless of the concealed dangers, once again remind of Heidegger's growth of saving power where danger lies. Hence, every entrepreneur will decide for themselves whether it is lucrative or not to transfer the business[134] to blockchain. Politicians will decide whether it is for their state's benefit to translocate the public administration and the entire democratic process to blockchain (for example, Estonia has transferred million healthcare records to a blockchain system).[135] Judging by the transfer of the paradigm to the digital platform and the fact that the value of the trust will have a significant role on that platform,[136] blockchain appears as the perfect candidate for accomplishing such plans.

3.4. Corruptive Elements of Blockchain Technology

I described how asymmetrical cryptography protects the ownership and data in the system, hindering false identity. Through the research on blockchain algorithm, I demonstrated the impossibility of accepting invalid transactional blocks, as they go through the process of verification in the whole system. For the same reason,[137] one cannot imagine the situation in which a certain node deliberately keeps information to itself, unwilling to forward it. Designing the communication between the nodes on the principle of gossip annuls the possibility of deliberate non-forwarding of the information. Regardless of whether we intentionally overburden certain node in order for it to stop working and competing in the system, the decentralised system continues its further work. The malfunction of one node does not affect the decentralised system due to its architecture. Although blockchain seems excellent from the technical point of view, we must not forget that it closely combines technical and non-technical aspects. The greatest vulnerability lies in the intention of people – for

what purpose will it be used. We can, therefore, separate the good from the bad intention of using technology.[138] Intention[139] is the most important feature, and speaking of the term, I will mention Aristotle[140] and the context in which he uses this term:

"But where there is no contract for the service, people who offer it for the sake of the other person, as we have said, cannot be complained about, since this is the nature of friendship based on virtue."[141]

One should keep in mind that Φιλια, apart from friendship, can also mean love and affection, while it most commonly represents any amicable sentiment between people; from the love between friends to the matters of business affinity. Some modern ethical approaches argue that love and intention of building a friendship is the key to prosperity.[142] In the case of blockchain technology that would translate that nodes in the system should also be "friends" and "care for each other". If we consider other approaches on business affinity, good intention is important but in the sense of cooperation, not building friendship, and it can lead to economic welfare.[143]

Bad intentions will lead to a deficit of cooperation and the emergence of corruption.[144] Corruption can dangerously damage the view of the public on any

132
D. Drescher, *Blockchain Basics*, p. 208.

133
Ibid., p. 219.

134
Some authors, for example Franco Berardi and Giuseppina Mecchia, criticise political and economical system we live in and believe that system, capitalism, is responsible for separation of the individual from their roots. That process is further intensified and accelerated by digitalisation. They believe that capital destroys the political and psychological ties that enabled its emergence and is focused on the circulation of digitised information. Cf. Franco Berardi, Giuseppina Mecchia, "Technology and Knowledge in a Universe of Indetermination", *SubStance* 36 (2007) 1, pp. 57–74, p. 67.

135
Ian Allison, "Guartime Secures over a Million Estonian Healthcare Records on the Blockchain", *IB Times* (4 March 2016). Available at: http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367 (accessed on 13 September 2020).

136
Richie Etwaru, "TEDxTalks: Blockchain Massively Simplified", *YouTube* (15 May 2017). Available at: https://www.youtube.com/watch?v=k53LUZxUF50&t=51s (accessed on 13 September 2020). Cf. P. Vigna, M. J. Casey, "Decentralized Economy with Centralized Trust", in: P. Vigna, M. J. Casey, *The Truth Machine* [Freda, EPUB format].

137
This refers to the concept of *blockchain algorithm*.

138
Cf. Jorris Vlieghe, "Education in an Age of Digital Technologies. Flusser, Stiegler, and Agamben on the Idea of the Posthistorical", *Philosophy and Technology* 27 (2014), pp. 519–537, doi: https://doi.org/10.1007/s13347-013-0131-x.

139
Greek προαίρσις means choice, but also intent (lat. *intentio*); for the purposes of this paper I translated it as – intention.

140
I. Kant, "Second Section – Transition from popular moral philosophy to the metaphysics of morals", para. 15, in: I. Kant, *Fundamental Principles of the Metaphysic of Morals* [Freda, EPUB format]. Kant is of the opinion that the moral law directly determines the will and, if we do good, our will and intentions are always good.

141
Aristotle, *Nicomachean Ethics*, 1164a.

142
Manuel G. Velasquez, *Business Ethics Concepts and Cases*, Pearson Education, Essex 2014, pp. 125–130.

143
Johan J. Graafland, *Economics, Ethics and the Market*, Routledge, New York 2007, p. 242.

144
Ibid., p. 244.

technology, not just blockchain ,and lead to deterioration of conception and practice. Some authors, however, go further and argue that the system itself is corrupt and cannot be fixed from the inside.[145]

In the next subchapters, I will briefly demonstrate weaknesses of the blockchain technology.

3.4.1. 51% Attack[146]

When talking about reaching a consensus on the unique history of data transaction, we have to keep in mind that every node has the right to vote (*voting schema*). Here, the majority decides on something fundamental for the functioning and performance of any platform based on blockchain technology. If one or more people pursuing their interest try to control the history of data transaction in a manipulative manner, these actions are called, in the domain of blockchain algorithm, i.e. the way this technology functions, *a 51% attack*. I previously mentioned that this kind of manipulation is costly since it would be necessary to alter the entire history of data transaction to the so-called root block in the Merkle tree, but it is theoretically possible.[147] If such manipulation occurs, the scenario could emerge in which one person, or an interest group, controls the entire network and acts by their own will:

"Let's say some wealthy despot has decided that bitcoin, like the Internet before it, has become so influential that it is eroding his power. This despot could seize all the mining power within reach and purchase the rest from countries that still tolerate his bad behavior, to put him over the 50 percent hash rate threshold. He could then decide which transactions to include in blocks and which to reject. With controlling interest, he could also decide whether to fork the code and introduce a few prohibitions (...)."[148]

From the economic aspect, the attackers want to alter the history of data transaction to ensure larger property for their benefit. Regarding the collective decision making, this manipulation intents to produce the final result that would be beneficial for the attackers if there should be a joint decision on a certain matter. From the technical aspect, the attack aims to destabilise or destroy integrity and trust within the system, make it unsustainable and ultimately meaningless. Should we tackle the problem from the point of centralisation, then this kind of attack can alter the architecture of the system and introduce hidden centrality. The key solution is to control the majority[149] in order for the potential attack to be successful, and as this minimum amounts to 51%, this problematic was named accordingly.[150] However, if an individual or a group are given an opportunity to control the technology that is essentially designed to belong to the decentralised network, this is considered unjust.[151] If this is unjust, then it does not correspond to justice[152] that represents the highest virtue.[153] Subjecting oneself to injustice is in nobody's interest[154] and according to A. Tapscott and D. Tapscott, avoiding this kind of future scenario is unlikely to happen.[155] Mentioned problem, without any doubt, represents a challenge to the *blockchain* technology. The only solution offered so far is that the whole process will be too expensive for the potential attackers and that, for this reason, they will abandon their plans before they even commenced planning.[156]

3.4.2. Other Corruptive Elements

The entrance of new members into the decentralised system of peer-to-peer computer network based on blockchain technology is encouraged. Block-

chain is available to everyone and gladly accepts new nodes into the system. In short, it is transparent. The transparency principle is useful because multiple users can verify executed transactions, and it is much easier to detect and correct the *double-spending* problem. On the one hand, if we operate in permissionless blockchain system, all transactional data are available to everyone, so the ownership is quite safe,[157] while there can be on objection regarding lack of privacy. On the other hand, if we decide to limit the access and accept only certain nodes, the principle of transparency is being annulled, and there is a possibility of developing private blockchain systems. At this point of discussion, we can ask ourselves how much sense it makes to develop multiple blockchain systems that are private versus transparent. On the one hand, blockchain guarantees the security of the ownership data and enables direct communication among all the users while interfering with privacy on a higher level.[158] On the other hand, it enables the access only to certain, selected members where lack of nodes equals less stabile system that is more likely to be subject to the 51% attack.

Responsibility[159] can also be considered a potentially corruptive element in blockchain technology. For example, in modern transactions, it takes at least

145
"Virtual capitalism is perpetually failing behavioral organisms, placing them in a state of permanent insecurity. When virtual capitalism creates insecurity through its perpetual displacements, (recombinant) fascism comes in to mobilize the hatred for existence." – Arthur Kroker, Robert Weinstein, *Data Trash*, St. Martin Press, New York 1994, p. 65. Some authors do not see the problem in the intention, they criticise virtual capitalism and argue that the system in general is corrupt. Blockchain technology would only add to that corruption from this perspective.

146
51% attack is possible in the specific blockchain system that has been researched here – decentralized blockchain with peer-to-peer computer network based on distributed ledger.

147
M. Swan, *Blockchain*, p. 66.

148
A. Tapscott, D. Tapscott, "Powerful incumbents of the old paradigm will usurp it", para. 6, in: A. Tapscott, D. Tapscott, *Blockchain Revolution* [Microsoft Edge, EPUB format].

149
M. Swan, *Blockchain*, p. 83.

150
Cf. D. Drescher, *Blockchain Basics*, p. 178.

151
If we presume that blockchain is used in the imperfect markets where businesses thrive against each other in unjust setting than it could mean, contrary to what one would assume, opportunities for business growth. Cf. Prakash Sethi, "Imperfect Markets: Business Ethics as an Easy Virtue", *Journal of Business Ethics* 13 (1994) 10, pp. 803–815, pp. 807–808, doi: https://doi.org/10.1007/bf00876261.

152
Aristotle, *Nicomachean Ethics*, 1129a.

153
Ibid., 1129b.

154
Ibid., 1136b.

155
A. Tapscott, D. Tapscott, "Powerful incumbents of the old paradigm will usurp it", para. 6, in: A. Tapscott, D. Tapscott, *Blockchain Revolution* [Microsoft Edge, EPUB format].

156
Ibid., para. 7 [Microsoft Edge, EPUB format].

157
D. Drescher, *Blockchain Basics*, p. 214.

158
Ibid., p. 245.

159
"We are not used to governance being a personal responsibility and a peer-to-peer system as opposed to something externally imposed by a distant centralized institution. We are not used to many aspects of blockchain technology (…) but we learn appropriate savviness and new behaviors and conceptualizations when adopting new technologies. We are not used to decentralized political authority and autonomy." – M. Swan, *Blockchain*, p. 52.

two people that represent, let us say, two public limited liability companies on the labour market, that have found a point of interest and would like to cooperate. They sign an agreement and resolve possible disputes by legal actions. If we completely transfer carrying out transactions to the blockchain technology (what is possible because it annuls mediation), there would be no need for meetings and signing the physical contracts. However, if we put all of our trust in this technology and rely on it entirely, this might mean the lack of responsibility. It can undoubtedly be stated that smart contracts from the technical side solve the problem. However, so far, there is no strict legal framework that would regulate smart contracts, because that would mean shifting the whole paradigm of jurisprudence to the digital platform, and thus we can state that there is also a solution from the legal point of view that lies in the regulation of the laws on obligation on the digital platform and in the adoption of additional acts regarding blockchain technology. However, by actualising this scenario we have not even touched the question of transferring the responsibility to technology and accepting, i.e. denying responsibility because the subject in question is placed in a digital, not to say the abstract world, detached from reality.[160]

There are teams of people who offer the answers to certain questions raised in this work by concrete projects.[161] For this reason, it is daunting to predict the future. This technology is still a novelty, and there are many questions, aspects or segments of this technology and its effect on the society is yet to come. Through the positive application, I have demonstrated that we can build significant and useful projects based on blockchain, by respecting the inbuilt moral values. To reaffirm – *techne* and *physis* are incredibly close in the *blockchain*. If we merge that fact with the statement that morals radiate from blockchain, in the conjunction of the technical and non-technical, morals will appear as a copula, as a binding substance that connects the two.[162] At the moment, it is difficult to perceive the concept of morals, what will become almost extravagant when some new, never before seen questions arise that are connected to morals and come from the digital platform. For example, is it morally justified to take down the blockchain system that archives the data about euthanised people in a certain hospital? Or, is it morally justified to trade in cryptocurrency that hides transactional data and can be used as a means of buying weapons?[163]

To conclude: moral challenges will continue to exist, but they will, in a growing number of cases, arrive from the digital platform. There is no indication that moral values would disappear or transform themselves into something unknown or unseen, but they will increasingly appear in dichotomy with technology through the change of context.

Conclusion

I am convinced that blockchain itself will represent the key technological innovation in the future, as it was once the case with the Internet, or prior invention of television or the radio receiver and that with time people will understand the benefits it offers. Despite all the efforts to norm the positive values and emphasise the virtues through education, decisions will still be made by the individuals.

It is frequently the case that engineers who work on developing possible applications of the blockchain technology and enhancing its features simultane-

ously act as ethical regulators. They aim to create a system that would ensure trust and integrity to establish security firmly. They do that in innovative technical surroundings with the presumption that the level of trust in the system is minimal. Nothing more or less, the suggestion is to work on these virtues, which is why an emphasis is put on virtue ethics. At the beginning of this paper, the definition was arbitrary, but I noticed by sole analysis of the incredible similarities between the blockchain system and Platonic and, above all, Aristotelian teaching on virtues. From the rational perspective, virtue ethics is imposed as a model compatible with the reaches of the blockchain technology and can offer the suggestions that would have a positive impact on the application on the blockchain in the future.

This paper is a small contribution to the beginnings of the blockchain research, and I hope it will encourage further debates and analyses, even some argued opinions that are opposite to the ones presented in this paper.

Jurica Marković

Etički temelji tehnike *blockchaina*: uvodno razmatranje

Sažetak

U radu se sažeto objašnjava tehnika blockchaina *i daje pregled temeljne moralne problematike vezane za njenu tehničku primjenu te postojeću i moguću društvenu ulogu. Tijekom istraživanja, etika vrlina pokazala se kao najkompatibilnija za razumijevanje i opisivanje tehničkog fundamenta* blockchaina *i razmjera njegove primjene.*

Ključne riječi

blockchain, tehnika, etika, etika vrline, kriptovaluta

160
By transferring responsibility to technology people make a conceptual mistake because technology is not and cannot be a moral subject. – P. Brey, "Values in technology and disclosive computer ethics", p. 87.

161
"In recent years, many technology start-ups have emerged that are working on blockchain projects and are offering solutions specific to this technology. There is a significant increase in the number of start-ups that are offering blockchain consultancy and solutions." – I. Bashir, *Mastering Blockchain*, p. 584. There are more than 5300 blokchain startups. Data Available at: https://angel.co/blockchains (accessed on 28 October 2020).

162
"There was a time when it was not technology alone that bore the name techne. Once that revealing that brings forth truth into the splendor of radiant appearing also was called techne. Once there was a time when the bringing-forth of the true into the beautiful was called techne. And the poiesis of the fine arts also was called techne." – M. Heidegger, *The Question Concerning Technology and Other Essays*, p. 34.

163
Cf. Kenneth Einar Himma, "Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking", in: Kenneth Einar Himma, Herman T. Tavani (ed.), *The Handbook of Information and Computer Ethics*, John Wiley & Sons Inc., New Jersey 2008, pp. 206–216. The reader is advised to read further on questions of moral justifications on computer hacking for the cases of digital intrusions.

Jurica Marković

Ethische Grundlagen der *Blockchain*-Technik: eine einleitende Überlegung

Zusammenfassung

In der Arbeit wird die Technik der Blockchain *gerafft erklärt und ein Überblick gegeben über die grundlegende moralische Problematik im Zusammenhang mit ihrer technischen Anwendung sowie mit der bestehenden und möglichen gesellschaftlichen Rolle. Im Laufe der Forschung erwies sich die Tugendethik als die kompatibelste für die Erfassung und Beschreibung des technischen Fundaments der* Blockchain *und des Ausmaßes ihrer Anwendung.*

Schlüsselwörter

Blockchain, Technik, Ethik, Tugendethik, Kryptowährung

Jurica Marković

Les fondements éthiques de la technique du *blockchain* : considérations liminaires

Résumé

Ce travail explique de manière succincte la technique du blockchain *et donne un aperçu de la problématique morale liée à son application technique, mais également à son rôle social actuel et possible. Au cours de la recherche, l'éthique de la vertu s'est avérée être la plus pertinente pour comprendre et décrire le fondement technique du* blockchain *et l'étendue de son application.*

Mots-clés

blockchain, technique, éthique, éthique de la vertu, cryptomonnaie