DOI 10.5817/MUJLT2022-1-3

BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE: CONNECTING TWO DISTINCT TECHNOLOGIES TO COMPLY WITH GDPR'S DATA PROTECTION BY DESIGN PRINCIPLE

by

DÁNIEL ESZTERI*

The aim of the paper is to present some of the general principles of data protection law that can be applied to automated decision-making applications embedded into blockchain technology in order to comply with the provision of the European Union's General Data Protection Regulation (GDPR). The analysis focuses on the applicability of the 'data protection by design' principle during the development of such systems. Because blockchain-based networks are built on distributed data processing operations, therefore data controlling or processing of participating nodes should comply some abstract data protection patterns predetermined and collectively built-in during the system's development phase. On the other hand, the imprint of AI's automated data processing could be also observed and tracked back in the blockchain due to its historically retroactive nature. In the end, the study presents the human mind and its 'uploading' with conscious and unconscious contents as an analogy to blockchain-based AI systems. My goal is to highlight that the synergy of blockchain and machine learning-based AI can be hypothetically suitable to develop robust yet transparent automated decision-making systems. The compliance of these distributed AI systems with data protection law's principles is a key issue regarding the high risks posed by them to data subjects rights and freedoms.

* daniel.eszteri@outlook.com, Head of Data Breach Notification Unit at the Hungarian National Authority for Data Protection and Freedom of Information, lecturer in data protection law at Eötvös Loránd University Faculty of Law and National University of Public Service, Hungary.

KEY WORDS
General Data Protection Regulation, GDPR, Blockchain, Artificial intelligence, Machine learning, Automated decision making, Data protection by design

1. INTRODUCTION

Blockchain (a distributed data processing network technology) and artificial intelligence (AI) are two fields of technological developments that are being heavily discussed in legal scientific literature nowadays. As of now legal literature tends to examine these topics separate from each other.

However, these innovations can be applied jointly and will likely converge in the future. One possible connection between these technologies could be that blockchain provides the infrastructure for data processing and sets up the rules of engagement, while AI optimizes processes and rules. Data can be collected by IoT devices or just simply loaded into the system by the data controller as an already available training database.

In my paper I would like to identify and examine the connections of these apparently remote topics in order to strengthen the discussion on them in terms of the European Union's General Data Protection Regulation (GDPR). In the analysis I take it as a prerequisite that personal data should be processed in the blockchain and some kind of automated decision--making mechanism should be also present with the personal data without human intervention. With the creation of a system like this, the concept of blockchain-based AI can be made which can heavily affect the fundamental rights and freedoms of data subjects.

Blockchain-based data processing systems equipped with AI could pose a risk to the rights and freedoms of individuals because they could be built around two quite new and less mature technologies. In the first part of the study the nature of the two examined technologies will be presented from a data protection point of view, then in the second part, I shall attempt to present the problems stemming from the connection of the technologies.

2. NATURE OF DATA PROCESSING BASED ON BLOCKCHAIN TECHNOLOGY

2.1 BLOCKCHAIN AS A NETWORK FOR DATA PROCESSING

Blockchain-technology is a representative of the so called 'distributed ledger technologies', which was also frequently implemented into real practice

during the last decade, mostly in the form of cryptocurrency networks. Distributed ledger is a transactional database which is distributed on a network of more computers thus it is not stored in a central place. The term blockchain stems from the attribute of the system that transactions are stored in groups in the so-called blocks. The blocks form a chain connected to each other in chronological order.[1]

Blockchain can be described, in an intentionally simplified way, as a data storing and authenticating system. Prerequisite of this data storing and authenticating system is a distributed network consisting of computers with no subordination or superiority to each other. Computers connected to the distributed network function as 'nodes' which are also connected with each other. In the end, every node is connected somehow to all of the others. The advantage of this network is that disconnection of a node does not make any disruption in the system, because their tasks can be taken over by any other node.[2]

Data packages in the blockchain can be suitable to store any type of information so the technology can be used universally for nearly any kind of data processing purpose.[3]

2.2 THE BLOCK AS A UNIT FOR STORING DATA

In networks built on blockchain technology data is stored in the so-called blocks. According to some views, blocks can be seen as a blank paper, document or board to which any information can be written.[4]

Thus, we can treat a block in the moment of its creation as "tabula rasa" based on the concept of empiricist philosophy. With this concept, philosophers of the empiricist school wanted to convey that the human mind – as some kind of information processing medium – does not include any inborn, original knowledge at the moment of birth.[5] On the contrary,

---

1 European Central Bank. (2017) *How could new technology transform financial markets? 19th April 2017.* [online] Available from: www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.en.html [Accessed 08 February 2021]

2 Győrfi, A. et. al. (2019) *Kriptopénz ABC (Cryptocurrency ABC).* Budapest: HVG Books, pp. 57-59.

3 For example blockchain can be used as a good tool for identity management purposes. In: Shraddha, K. (2018) Building-Blocks of a Data Protection Revolution – The Uneasy Case for Blockchain Technology to Secure Privacy and Identity, *Munich Intellectual Property Law Center - MIPLC Studies*, Vol. 35., 1. Edition 2018, Available from: doi.org/10.5771/9783845294025 [Accessed 11. November 2021], pp. 31-33.

4 Győrfi, A. et. al. (2019) op. cit., p. 60.

5 See e.g. Aristotle (in "On the Soul") and later in the Enlightenment John Locke ("An Essay Concerning Human Understanding"). In.: Andrássy, G. (2008) *Philosophy and Legal Ethics*. Dialog Campus, Pécs, pp. 32-33, 67.

representatives of the school of rationalist philosophy are on the standpoint that the mind of every human being includes some predetermined ideas or patterns that are present from the moment of birth in its deeper layers.[6]

Depending of the purpose of the given blockchain's creation, blocks as data storing units can store any kind of data and related information. Blocks storing information are connected to each other in a chain-like, posteriorly unchangeable way, which means that new blocks containing new data are always being connected to the end of the chain. The first created block in the beginning of the chain is called the 'genesis-block'.[7]

Regarding data processing, there is no actual data transfer between blocks in the blockchain network. This means that the execution of data processing operations with data stored in the blocks happens so that the network only assigns the 'right of disposal' to the given dataset. Technically speaking, the network assigns the 'digital signature' (via hashing) of users to the stored datasets and decides this way that who will have the right to disposal, access etc. on the given data.[8]

The network is built up like a chain and new data is added in newly created blocks which constitutes the ever-growing network of the blockchain. The log and hashes of every data processing operation is also stored in the individual blocks alongside the data itself (the summary of transactions results in the so called Merkle-tree).[9] The history of data processing operations is called the 'block-history'.

The algorithmic verification of every single data processing operation with the data stored in the blocks is the task of the computers (the nodes) connected to the network.[10]

During the approval of an operation, the following two elements will be verified by the nodes: Is the operation appropriately signed with the digital

---

[6] See for example Plato's thoughts on the world of ideas (in "Parmenides") at the earliest, and later, for example, Descartes takes a position in favour of rationalism against the concept of tabula rasa (in "Discourse on the Method"). In.: Andrássy, G. (2018) op. cit., pp. 35, 73.

[7] Győrfi, A. et.al. (2019) op. cit., p. 61.

[8] Hungarian National Authority for Data Protection and Freedom of Information. (2017) Opinion on Blockchain Technology in the Context of Data Protection (18th July 2017). Available from: *https://naih.hu/data-protection/decisions* [Accessed 08 February 2021], p. 3.

[9] Frankenfield, J. (2021) Merkle Root (Cryptocurrency). Available from: https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp [Accessed 22 December 2021]

[10] Kakavand, H. et. al. (2017) The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 [Accessed 13 February 2021], pp. 4-7.

signature of the initiating party and does it have any authentic previous history on the blockchain.

If the nodes (or a predetermined number of them) approve the operation, than it is recorded in the block which will be stored in the chain in an unchangeable way. Further guarantee of credibility is that every single node will download a copy of the blockchain in order to continuously monitor each other for verification purposes and to share the newest copy of the database with each other.[11]

Based on the information above, we can describe blockchain in the simplest way as a data processing technology that enables processing of data on a joint, distributed network which is functional without the existence of any central verification body. The verification of data processing operations on the network is ensured by algorithmic based self--checking mechanisms.

3. ESSENTIAL CHARACTERISTICS OF MACHINE LEARNING TECHNOLOGIES AND THEIR CONNECTION WITH BLOCKCHAIN

3.1 GENERAL TECHNOLOGICAL BACKGROUND OF MACHINE LEARNING

I would like to highlight and present the technological background of AI and machine learning only to the extent, that is necessary to understand and analyse the model of blockchain-based AI and ML from a legal point of view.

The report of the Norwegian Data Protection Authority (Datatilsynet) describes AI as a system capable of learning based on its own experience and to apply the knowledge obtained in different situations to resolve complex problems. The heart of the concept is that AI learns from the personal data it 'sees' (in practice the input data) and makes decisions or 'forecasts'.[12]

AI on the other hand serves as an umbrella term, which covers all the procedures when a software makes a decision automatically.[13] Relative

[11] Győrfi, A. et.al. (2019) op. cit., pp. 63, 68.

[12] Datatilsynet. (2018) Artificial intelligence and privacy. Available from: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf [Accessed 8 February 2021].

[13] Commission nationale de l'informatique et des libertés (CNIL) (2017). How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence. Available from: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_

to this, machine learning (ML) is a narrower concept, which means one branch of AI development. The heart of this is that the system generates independent knowledge out of its own experience.[14] Based on data examples and patterns, the system is able to recognise and determine regularities and rules independently or with human assistance and then makes decisions based on the regularities discovered in the acquired knowledge base.[15]

Data processing carried out by an AI system in the course of ML can be divided into three steps as follows:

(1) First, a large quantity of data is input in the system and the algorithm tries to find patterns and similarities in this data set. If the algorithm finds identifiable patterns, it will record and save them for subsequent use. After this, the system generates a model on the basis of the recorded and saved patterns. Based on the already identified patterns, with the help of the model, the system is capable of processing the subsequently input data.

(2) After this, the AI system operates as follows: first, new data are uploaded in the system, which are similar to the data used for learning. Then, based on the model, the AI decides which new data are similar to which learned pattern.

(3) Finally, the system makes a decision based on the acquired patterns with the new input data and informs the observer about the decision.[16]

It is also important to note that the model generated in the course of machine learning does not necessarily contain the source data, which served as the basis of its learning. In most cases, the AI system generated in the course of ML is able to operate independently of the data that served as the basis of learning.[17]

---

gb_web.pdf [Accessed 23 July 2021], pp. 16-17.

[14] Szepesvári, C. (2005) Machine learning – a brief introduction. [lecture] MTA SZTAKI. Available from: http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf [Accessed 9 February 2021].

[15] European Union Agency for Fundamental Rights. (2019) Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights. Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf [Accessed 22 July 2021], pp. 4-5.

[16] Datatilsynet. (2018) op. cit., p. 7. and European Union Agency for Fundamental Rights (2019) op. Cit., pp. 4-5.

[17] Datatilsynet. (2018) op. cit., p. 10.

Characteristically, ML requires a much larger quantity of raw data than the human brain does in order to be able to efficiently identify patterns and to set up decision-making models on their basis. So, at first, we might think that the more data we have, the better AI systems based on machine learning we can produce. Yet, the quality of the data used for machine learning, their appropriate prior selection and labelling are much more important aspects. Even before inputting the data in the system, it is necessary to clarify the exact purpose of using the data to carry out specific tasks and because of this, the range of the data used must be restricted to those relevant for the given purpose. The good selection and preliminary choice of the data used is also a very important criterion.[18]

3.2 AUTOMATED DATA PROCESSING ON THE BLOCKCHAIN NO 1.: SMART CONTRACTS

Researchers dealing with distributed ledger systems already described the possibility of automatization of data processing operations in the blockchain by running algorithms on the network.

It was Nick Szabo who described for the first time – using the concept and term of "smart contract" in 1996 –, the automatization of data processing operations in a distributed network. According to Szabo, a smart contract is such a contract that is being automatically fulfilled if its previously specified conditions are met, therefore the contract is unbreachable. When the contractual conditions are met, than the fulfilment, security and inviolability of the contractual terms are being secured by the computer network in which the parties created it. Therefore, the contracting parties do not need to rely on the assistance of a third party, for example a lawyer, for authentication.[19]

As it can be already seen in practice, blockchain is a fully viable technology for running smart contract applications: the possibility for users to enter into smart contracts was introduced by the blockchain-technology--based platform, Ethereum.[20] In essence, the program running on the network automatically executes a certain decision when the required conditions are met.

In the case of smart contracts, the verification of the operations and

[18] Datatilsynet. (2018) op. cit., p. 11. and European Union Agency for Fundamental Rights (2019) op. cit., pp. 10-12.

[19] Szabo, N. (1996) Smart Contracts: Building Blocks for Digital Markets. Available from: www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf [Accessed 8 February 2021], pp. 1-5, 8.

[20] Buterin, V. (2013) A Next-Generation Smart Contract and Decentralized Application Platform. Available from: https://ethereum.org/en/whitepaper [Accessed 14 February 2021].

the processed data is the task of the network nodes. Verified data can be, for example, the bank account number of contracting parties, the amount, relevant dates (e.g. deadlines), other terms, related personal data (e.g. names), and even other textual information (e.g. statement, short message) could be recorded. Therefore, a smart contract embedded in blockchain is dependent on outside input. Data, executed operations and other information relevant in the context of the contractual conditions are recorded and logged in the blockchain in an unchangeable way.[21] According to a more technical perspective, for example, the hash of a file and the owner's name can be stored as pairs in the code to achieve the functionality of proof of ownership. The hash of a file and the block's timestamp can also be stored as pairs to realize the proof of existence function.[22]

The smart contract application runs on every node of the distributed network, so every user can benefit of it and use its functions. The code and algorithm of the smart contract application responsible for automatization is available, accessible and usable by every participant of the network.[23]

However, smart contract applications should not be mistaken with AI techniques. Smart contract applications cannot be treated as AI applications on their own, because they do not make individual decisions based on data in the blockchain. The main purpose of smart contracts in most situations is only to automatize and authenticate transactions on the blockchain when certain conditions met. In most cases do not feature a great deal of complexity.[24] Based on the above, AI and ML can enhance the efficiency of smart contracting applications but smart contracts are not considered AI themselves.

3.3 AUTOMATED DATA PROCESSING ON THE BLOCKCHAIN NO. 2.: A DISTRIBUTED AI?

Turning back to the blockchain as the starting point of our topic: if we would run an analyser software on the blockchain which is capable

---

[21] Filatova, N. (2020) Smart contracts from the contract law perspective: outlining new regulative strategies, *International Journal of Law and Information Technology*, Volume 28, Issue 3, Autumn 2020. Available from: https://doi.org/10.1093/ijlit/eaaa015 [Accessed 14 February 2021], pp. 220-222.

[22] Xing, B. and Marwala, T. (2018) The Synergy of Blockchain and Artificial Intelligence. Available from: http://dx.doi.org/10.2139/ssrn.3225357 [Accessed 23 July 2021], p. 3.

[23] Bacon, J. et. al. (2017) Blockchain Demystified. *Queen Mary School of Law Legal Studies Research Paper* No. 268/2017, p. 29.

[24] Schrepel, T. (2021) Smart Contracts and the Digital Single Market Through the Lens of "Law + Technology" Approach. European Commission. Available from: https://ssrn.com/abstract=3947174 [Accessed 26 December 2021].

to identify patterns in the stored data by ML techniques, than it could become suitable to also make decisions automatically.

I emphasize – as it was already covered in literature – that blockchain-based data processing can be assisted or enhanced via various AI techniques.[25]

In my opinion there are two possibilities to run AI applications on the blockchain:

(1) *The blockchain-based machine learning approach:* AI analyzes data processing operations in blockchain and tries to identify patterns. In this case blockchain means the storing form and source of the training data. The identified patterns constitute a model which can later be used to produce a decision based on the identified patterns and also to increase system efficiency. In this case, blockchain stored data should serve as and input for AI-based data processing.

(2) *The blockchain-based automated decision making approach:* AI executes data processing operations on the blockchain and tries to optimize decisions at the same time. In this approach decisions made by the AI algorithm should also be logged in the blockchain itself (in fact: in the block-history and Merkle tree), as it was indicated in chapter 2.2. of the paper. In my opinion, it could be also possible to store a copy of the logs of the decisions in a separate (not necessarily blockchain-based) database as well, but it is not fundamentally necessary for the working mechanisms of such systems.

A collection of projects on applications or software capable of making automated decisions with processed data in the blockchain can be found in recent research papers in the field.[26] Moreover, a collection of blockchain-based AI projects can be found in recent paper of Vasco Lopes and Luís A. Alexandre (for example using blockchain to store "robotic events").[27] According to them, blockchain-based automated decision making

[25] Xing, B. and Marwala, T. (2018) op. cit., pp. 6-8.

[26] See, for example, the following study on the concept of blockchain-based profiling for energy management purposes: Sankaran, S. et. al. (2018) Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* Vienna.

[27] Lopes, V. and Alexandre, L. A. (2019) An Overview of Blockchain Integration with Robotics and Artificial Intelligence. *Ledger Journal Vol. 4, Supplement 1 (2019): Proceedings of the First Symposium on Blockchain and Robotics,* MIT Media Lab, Cambridge, MA, 5 December 2018, USA. Available from: https://doi.org/10.5195/ledger.2019.171 [Accessed 23 July 2021].

applications search patterns in the database and make decisions based on the identified model.

In this paper I consider as a prerequisite that purely automated (algorithm-based) decisions are made with personal data stored in the blockchain without any human intervention.

3.4 EXAMPLES ABOUT THE SYNERGY OF BLOCKCHAIN AND AI

A good model can be found in the paper of Sandner et. al. about the synergy of blockchain and AI: in the hypothetic example a network of street lamps in a smart city constitutes the blockchain and every lamp has its own identity (block) on the network. Since all lamps are connected to a blockchain they will store data about their usage, performance and downtime. AI could analyse this data and optimize the network's maintenance. For example suggests a more regular maintenance of more frequently used lamps etc.[28]

We can apply this example to a more personal data processing based system: for example, in Article 29 Working Party's (WP29) opinion, smart grids and smart metering has been already analysed from a data protection point of view.[29] The antecedent of the opinion was the European Commission's recommendation on preparations for the roll-out of smart metering systems. In the context of the recommendation smart grid means "an upgraded energy network to which two-way digital communication between the supplier and consumer, smart metering and monitoring and control systems have been added." Furthermore smart metering means "an electronic system that can measure energy consumption, adding more information than a conventional meter, and can transmit and receive data using a form of electronic communication."[30] Smart meters can actually be considered as a digital version of conventional meters, except that smart

[28] Sandner P. et. al. (2020) Convergence of Blockchain, IoT, and AI, Front. *Blockchain 3:522600.* Available from: https://doi.org/10.3389/fbloc.2020.522600 [Accessed 11. November 2021.], p. 4.

[29] Article 29 Data Protection Working Party. (2013) Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP209). Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf [Accessed: 25 November 2021].

[30] European Commission. (2012) Recommendation on preparations for the roll-out of smart metering systems (2012/148/EU) 9 March 2012. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012H0148& [Accessed: 15 December 2021], Article 1(3), (a)-(b).

meters act as a two-way communication channel between consumers and service providers (e.g. electricity, water, gas). The advantage of smart meters is that they transmit detailed and real-time consumption information to the provider in a simple and direct way. Consumers will receive a very detailed statement of their energy consumption based on real-time quantitative data, which will make their consumption easily optimisable.

The recommendation and the opinion already drew high attention to the requirements and enforcement of the principles of 'data protection by design and default' in the context of the planning and operation because huge amount of personal data about the consumers will be processed in such systems.[31]

If we apply the above mentioned hypothetic example of Sandner et. al. (blockchain-based street lamps) to a smart grid and smart metering system, we can say that individual households could constitute the blocks of the network. They can store data about their consumption of water, gas, electricity etc. and send it real time to the service providers. On the other hand AI and ML technologies could also analyse the consumption data of households and identify 'consumption-patterns' in order to optimize energy distribution between customers. Individual service providers could also share the identified data-processing patterns with each other to synchronize their services for a better service distribution.

In such systems, the history of consumption data will be recorded in the blocks (households) as well and can be tracked back historically. The effectiveness of consumption optimization by ML can also be followed in the blocks by tracking back consumption details of individual households. This could also make the system more transparent and help to develop further the applied AI and ML techniques for a better functioning smart grid and smart metering system.

The recent report prepared for the European Commission and the European Investment Bank also took note that in the energy sector the synergy of these technologies can be used: AI to optimise energy use in the buildings and blockchain to share data to across the energy industry to optimise network usage.[32]

---

[31] European Commission (2012) op. cit., Article 1(3), (d)-(e).

[32] Verbeek A. and Lundquist M. (2021) Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy. Available from: https://op.europa.eu/en/publication-detail/-/publication/8730fef5-315c-11ec-bd8e-01aa75ed71a1/language-en [Accessed 21 December 2021], p. 109.

4. DATA PROTECTION ISSUES OF THE BLOCKCHAIN – AI SYNERGY

4.1 RULES ON AUTOMATED DECISION-MAKING IN THE GDPR

The GDPR, does not define the concept of *automated decision-making*, however it uses this expression several times in the normative text. On the other hand, the concept of *profiling* is included in the list of definitions of Article 4.

According to this provision, profiling means any form of automated processing of personal data to evaluate certain personal aspects of a natural person. In particular to analyse or predict the natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[33]

According to the relevant guidance of Article 29 Data Protection Working Party (WP29), automated decision-making is a capability of making decisions with the help of technological instruments without human intervention.[34] That is to say, there is no human involvement in decision-making in the case of exclusively automated decision-making.

Pursuant to Article 22(1) of GDPR, the data subject shall have the right not to be *subject to a decision* based *solely on* automated processing, *including profiling*, which produces *legal effects concerning him or her or has similarly significantly impact on him or her*. This provision constitutes a general prohibition on decision-making based exclusively on automated data processing. The regulation includes profiling based on such a decision--making process. This prohibition stands irrespective of whether or not the data subject takes any measure concerning the processing of his/her personal data. Therefore, as a main rule GDPR sets forth a general prohibition on exclusively automated individual decision-making, which produces legal effects or similarly significant impact.[35]

In order to qualify an activity as human intervention with regard to the decision and therefore the general prohibition of Article 22 should not apply to it; the controller has to ensure that the human review of the decision be of merit and not only a symbolic gesture. It has to be done

---

[33] GDPR Article 4(4).

[34] Article 29 Data Protection Working Party. (2017) op. cit., p. 8.

[35] Veale, M. and Edwards, L. (2018) Clarity, surprises and further questions in the Article 29 Working Party draft guidance on automated decision making and profiling. *Computer, Law and Security Review 34(2),* p. 400.

by a person, who has the authority and the competence to alter the decision. In other words, to be exempt from the prohibition, the final decision must be made by a human, or the decision proposed by the algorithm has to be reviewed and approved by them.[36]

Furthermore, the rules applicable to exclusively automated decision--making have to be applied only in the cases when the decision has legal effects or similar significant impact on the natural person. GDPR does not define the notions of "legal effect" or "similarly significant", but this wording of the regulation makes it clear that Article 22 extends only to effects involving severe consequence.[37]

The legal effect requires that the decision should influence the legal rights of a person. A legal effect may be something that will influence the legal standing of a person or his/her rights based on contract. According to WP29, examples of such effects include automated decisions concerning natural persons as a result of which: contracts are terminated, welfare benefits (such as child-related benefits or housing support) guaranteed by law are granted or rejected, entry to a country is refused, citizenship is denied etc.[38]

The effect of automated decision-making on the rights of people set forth in law or contract concerns cases that can be relatively clearly delineated. In addition, however, there is the more vaguely worded "similarly significant" impact in Article 22, which is also a circumstance subject to the prohibition. Recital (71) of GDPR may contain some guidance concerning this notion as it lists the following examples: "refusal of an online credit application" or "e-recruiting practices without any human intervention".

There are, however, exemptions from this general prohibition set forth in Article 22(2). Accordingly, the prohibition cannot be applied, if the decision is:

(1) necessary for entering into or performing a contract between the data subject and the data controller;

(2) authorised by European Union or Member State law, *to* which the data controller is subject and which also lays down suitable

[36] Article 29 Data Protection Working Party. (2017) Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01). Available from: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 [Accessed: 8 February 2021], p. 22.

[37] Veale, M. and Edwards, L. (2018) op. cit., p. 401.

[38] Article 29 Data Protection Working Party (2017) op. cit., p. 22.

measures to safeguard the data subject' rights and freedoms and legitimate interests; or

(3) based on the data subject's explicit consent: A clearest method of gaining assurance that the consent was expressed is a written statement of the data subject. According to the European Data Protection Board, in a digital or online context it may happen for instance that the data subject can issue the required statement by completing an electronic form, sending an e-mail or uploading a scanned document containing his signature or using an electronic signature. Finally, one can gain assurance of the validity of the express consent through the two-step control of the consent (a good example of this is the use of two stage verification).[39]

4.2 BLOCKCHAIN-BASED AUTOMATED DECISION MAKING AND THE GDPR

Therefore, where personal data is processed in the blockchain for automatic decision-making purposes, the controller must comply with the above requirements of the GDPR as well. Of course, it will always be the data processed, the specific purpose of the processing and its impact on the data subject that determines whether the rules of Article 22 applies or not. If so, data processing using automated decision-making is only possible on the blockchain if the controller can demonstrate the legitimate use of the exceptions above.

The common feature of applications running on blockchain that are capable of automated decision-making (including profiling in particular cases) should be that their decisions are based on the data processed in the distributed network and are free of any human intervention. In these cases Article 22 of the GDPR applies to such systems.

If we take the hypothetic example of blockchain-based smart metering from point 3.4. of the paper, in my opinion, such data processing falls under the ruling of Article 22, because automatic decisions influence the legal rights of persons (e.g. the right for electricity supply) and the processing is based on a contract between the data subject (customer) and the data controller (e.g. electricity service provider).

[39] European Data Protection Board. (2020) Guidelines on consent under Regulation (EU) 2016/679. Available from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [Accessed 30 December 2020], pp. 20-22.

4.3 COMPLIANCE WITH THE PRINCIPLES OF PURPOSE LIMITATION AND DATA MINIMIZATION

Blockchain-based data processing can cause serious confusion about its possible compliance with the GDPR's principles of purpose limitation and data minimization. On the basis of the purpose limitation principle, personal data should only be collected for a specific, clear and legitimate purpose and should not be processed further in a manner that is incompatible with those purposes.[40] According to the principle of data minimization, the personal data processed should be adequate and relevant for the purposes of processing and limited to what is necessary in relation to that purposes.[41] Both principles constitute a prohibition on the processing of exaggerated, stockpiling, unnecessarily handled and stored data.

One of the basic principles of blockchain is that all the data is stored in the database even after transactions or other operations with them are performed. Newer data processing operations will be connected via hashing to older ones to ensure integrity and security. More simply: data and transaction logs are supposed to be stored indefinitely in the system, so that one can accurately trace back individual data processing operations. The 'replicative' nature of the blockchain is also problematic from a data protection point of view when all nodes store a complete copy of the database for self-checking purposes.[42] At first sight, these characteristics are in contrast to the principles of the GDPR referred above.

However, it is a very important preliminary question for assessing the legality of blockchain-based data processing, that to what level the processing is compatible with the original purpose.[43]

Blockchain-based data processing can only comply with the principles of purpose limitation and data minimization if such type of processing of personal data (e.g. storing data in the chain) is compatible with the original purpose. There are types of data processing that are fundamentally not suitable for this. For example, data processing based on the consent of the data subject is almost never, since (at first sight), it is

[40] GDPR Article 5(1)(b).

[41] GDPR Article 5(1)(c).

[42] Finck, M. (2019) Blockchain and the General Data Protection Regulation. European Parliamentary Research Service, PE 634.445, p. 68.

[43] Finck, M. (2019) op. cit., p. 65.

impossible to carry out the obligation to delete personal data if the consent is withdrawn.[44]

However, in the case of data processing based on compliance with a legal obligation, such as the keeping of real estate registers[45, 46] or state archives, the situation is easier, since the purpose of these databases is to preserve and to keep accurate all personal data and all of the operations carried out with them.

Therefore, it is necessary to declare that a given blockchain-based data processing can only be assessed on a case-by-case basis from the perspective of legality and GDPR-compliance. Having regard to purpose limitation and data minimization, special attention should be paid to the selection of the appropriate legal basis for data processing. If the predetermined legitimate purpose of processing can comply with the specificities of blockchain technology, compliance with the principle of data minimization will not be problematic any longer.

If the controller wishes to use automatic decision-making algorithms for blockchain-based processing, of course, this processing operation must also be examined for compliance with the abovementioned principles.

In my opinion, if the purpose of data processing is legally compatible with the characteristics of the used technology, the operation of the automatic decision-making application using the data processed will be also compatible with it in most cases. The reason for this is that the data is stored in the blockchain itself, and automatic decision-making is only being 'built on' the database. Nevertheless, it is also important to examine the compliance of the system with the specific rules of the GDPR on automatic decision-making (see point 4.1. of this paper).

However, I stress that before loading data into the system, it is necessary to clarify exactly what kind of task the data is used for and therefore limit

---

[44] GDPR Article 17(1)(b): The data subject shall have the right to delete the personal data relating to him or her without undue delay at his request and the controller shall be obliged to delete the personal data relating to the data subject without undue delay if [...] the data subject withdraws the consent of the data subject on the basis of Article 6(1)(a) or Article 9(2)(a) and there is no other legal basis for processing.

[45] McMurren, J. et. al. (2018) Adressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers. Available from: blockchan.ge/blockchange-land-registry.pdf [Accessed 13 February 2021].

[46] Kachorowska, M. (2019) Blockchain-based land registration: Possibilities and challenges. *Masaryk University Journal of Law and Technology, Vol. 13. No. 2*. Available from: https://doi.org/10.5817/MUJLT2019-2-8 [Accessed 13 February 2021].

the range of data used to those relevant to the purpose.[47] This is also a key requirement for the application of the principle of data protection by design, which will be described later.

4.4 COMPLIANCE WITH THE PRINCIPLE OF TRANSPARENT DATA PROCESSING

One of the most frequently expressed concerns in relation to machine learning (and not only from the viewpoint of data protection) is that it is often impossible to predict what sort of result the system will produce. The model applied may produce a result, for which seemingly no explanation exists.[48] This phenomenon is referred to in machine learning as "black box". For an ordinary observer, the system works in practice by absorbing data on the input side, on the basis of which it learns something, then it produces some result. It is, however, extremely difficult to see why exactly it generated that result.[49]

The size of the network and the connections between the individual layers may render data processing tasks so complex that cannot be understood by humans, even data scientists. They just do not know what happens in the black box.

In scientific and technical fields, the black box is a device, system or object, which can only be examined on the basis of its input, output and transmission characteristics, its concrete internal operation is unknown, that is, its implementation is 'opaque' (black).[50]

Because of this, undertakings developing data processing based on AI solutions may be seriously challenged by the legal requirement of transparency in that regard.

The requirement that data processing must be transparent for the data subject (whose data are being processed) has been included among the principles of data protection for a long time. This principle is expressly named in the GDPR in Article 5(1)(a). Accordingly, personal data shall be

---

[47] Datatilsynet. (2018) op. cit. p. 11. and European Union Agency for Fundamental Rights (2019) op. cit., p. 10.

[48] Datatilsynet. (2018) op. cit., p. 12.

[49] Infostart. (2018) *Belenéztek a fekete dobozba az ELTE kutatói (Researchers of Eötvös Lóránd University looked into the black box)* [press release] Available from: https://infostart.hu/tudomany/2018/11/16/melytanulasi-halozatot-vizsgaltak-az-elte-kutatoi [Accessed 13 February 2021].

[50] Cauer, E. et. al. (2000) Life and Work of Wilhelm Cauer (1900–1945). *Proceedings of the Fourteenth International Symposium of Mathematical Theory of Networks and Systems (MTNS2000)*, p. 4.

processed lawfully, fairly and in a transparent manner in relation to the data subject. That is to say GDPR names the principles of lawfulness, fairness and transparency at the same time, hence they must be enforced in relation to every data processing operation with respect to one another and simultaneously.

A question therefore is how systems using machine learning can be set up so that they operate with sufficient transparency for the data subject from the viewpoint of the results they produce. The primary issue in relation to these data processing methods is whether it complies with the principle of transparency.

GDPR requires the controller to provide information in relation to decision-making based exclusively on automated data processing having legal effects or similarly significant effect. The regulation here also includes profiling based on such data processing.[51] Under this, the following three items of information must be communicated with the data subject:

(1) He must be informed of the fact of such data processing;
(2) He must be given information of merit on the logic applied; and
(3) Finally, he must be informed of the significance of the data processing and its expected consequences for the data subject.[52]

According to GDPR, controllers must provide "information of merit" on the logic applied. If a controller communicates only in general that it is, for example, "operating a system based on a neural network" may not be sufficient, as the data subject will have little idea of what is happening with his personal data in the course of processing.

The information of merit, however, does not necessarily mean that the controller should provide complicated explanations about the algorithm applied or present the algorithm in full. A detailed presentation of the technology would, in most cases, decrease the comprehensibility of the information and impede its reception.[53]

In addition to the above, it is necessary to note that the controller has to inform the data subject also about the "significance" and "expected consequences" of data processing. According to the WP29 guidelines, in order that this information be of merit and comprehensible, real and

[51] GDPR Article 15(1)(h).
[52] GDPR Article 13(2)(f).
[53] Attila Péterfalvi et. al. (2018) *Magyarázat a GDPR-ról (Interpretation of the GDPR)*. Budapest: Wolters Kluwer, p. 158.

tangible examples of possible effects should be given. In a digital context, controllers may also use additional instruments to present such effects and may apply visual techniques to explain a former decision. In such a case, the guidance gives the example of providing a comparable application.[54]

According to the joint research by the Oxford Internet Institute and the Alan Turing Institute of London, it may be also a good practice from the viewpoint of the transparency of the decisions made by the algorithms and the related data processing, when the controller provides an opportunity for the data subject to learn the operation of data processing by making available a test system for them.[55] In this way, the controller does not need to 'open the black box' to the data subject. It is sufficient, if it makes the data subject understand how the decision was made and what he can do in order to have a different (more favourable) decision in his case.[56]

In order to comply with the obligation of transparent data processing, the operation of a blockchain-based system may even be desirable. This is because all data processing operations in the blockchain are logged and stored in the database and are accessible to all nodes in the block-history. Of course, the log of operations stored in the blockchain contains only the results of the decisions, and not necessarily how the decision itself was made by the automatic decision-making software. However, all actions with the data can be studied by the users, which can make it easier to deduce or understand the logic behind the decision made by the algorithm.

5. APPLYING DATA PROTECTION BY DESIGN TO BLOCKCHAIN-BASED AUTOMATED DECISION--MAKING

5.1 IMPRINT OF DATA PROCESSING OPERATIONS IN THE BLOCKCHAIN

The GDPR mentions, among the general obligations of the controller and the processor, that they should incorporate various guarantees into the process in order to comply with data protection principles and the requirements of the regulation, as well as the rights of data subjects. These guarantees should cover appropriate technical and organizational

[54] Article 29 Data Protection Working Party. (2017) op. cit., p. 28.

[55] Wachter, S. et. al. (2018) Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology, 31 (2)*, pp. 863-871.

[56] Datatilsynet. (2018) op. cit., pp. 21-22.

measures that take into account the state of the art and the costs of implementation, the nature, scope, circumstances and objectives of the processing and the risks to the rights and freedoms of natural persons of varying likelihood and severity.[57] The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for the specific purpose of processing are processed. This obligation applies to the amount of personal data collected, the extent to which they are processed, the duration of their storage and their availability. In particular, these measures should ensure that personal data are not accessible by default to an unspecified number of persons without the intervention of the natural person.[58] These provisions of the GDPR are called the principle of data protection by design and by default, whose function is to take compliance with the regulation by default at both the technical and organizational level when designing systems for data processing.

Compliance with this principle is also necessary for blockchain-based personal data processing and automated decision-making applications based on it, so developers should always take a close look at the up-to-date techniques and organizational solutions available on the market and applicable to the technologies used.

This means that during the development and testing process of blockchain-based automated decision-making systems data protection compliance should be monitored and applied long before the start of live data processing. In this way data protection compliance would appear also when the live system begins to work in practice.

The following theory could be set up to follow the aforementioned principle: The block, as a data storage unit, may contain any (digitizable) personal data or information at the time it is added to the chain. The nature of the data and information processed can only be limited by the specific purpose. However, the operational principles of blockchain-based data processing will begin to be developed already before live personal data is added to the system. It is the responsibility of the controller and the processor to consider data protection compliance even in the early stage of development of the system, on the basis of the principle of data protection by design as described above. In doing so, it is necessary

[57] GDPR Article 25(1).
[58] GDPR Article 25(2).

to examine, inter alia, the requirement of purpose and storage limitation, or transparency as set out above, as well as the form of information provided to the data subject and the existence of a legal basis for automated decision-making. These are, of course, only steps on the path of GDPR--compliance because the controller should also consider compliance with the additional requirements of the regulation.

This is also important because the immutable storage of data and logging all of the data processing operations in the blockchain can serve as a kind of perpetual imprint for checking compliance (see for more details on processing point 2.1. and 2.2. of the paper). The indelible imprint of data processing operations in the blocks represents such processing patterns in which compliance with data protection law can be also examined. These patterns are available in all node-managed replicas of the blockchain. In my opinion, the imprint of these patterns can be also studied if the personal data are otherwise processed in a separate database using so-called off--chain solutions.[59]

5.2 IMPRINT OF AI'S OPERATION IN THE BLOCKCHAIN?

If automatic decision-making applications and algorithms are used in the blockchain-based system when processing personal data, the data processing operations carried out by such applications can be followed in the system's log (block history and Merkle tree). In my opinion the imprint of AI-made decisions with personal data can be followed and tracked back when AI executes data processing operations on the blockchain and tries to optimize decisions at the same time as it was indicated in point 3.3 of the paper ('blockchain-based automated decision--making approach'). In this approach decisions made by the AI algorithm should also be logged in the blockchain itself.

By examining the imprint, we could see the big picture of the decisions the algorithm is making with the data. By examining the patterns that each decision assembles, we could better understand the background of automatic decision-making and how the AI works. This may also be crucial for understanding the processes in the black box, which may ultimately facilitate information on the logic used in automated decision-

[59] Off-chain data processing is a blockchain-based technology in which personal data is stored in a separate database rather than in the blockchain itself, but is processed using hash keys to connect to the back-end core database, which is already blockchain-based. See: Mannan, R. et. al. (2019) GDPR and Blockchain: A Compliance Approach. *European Data Protection Law Review 2019(3)*, pp. 423-424.

-making and its importance and expected consequences for the individual, as set out in Article 13(2)(f) and Article 22 of the GDPR.

The design of the behavior of the blockchain-based distributed AI will be recorded in the blocks and will be collectively present in the data processing operations performed by all nodes. The main source about the imprint of the AI's operation could be the block-history.

I am of course aware, that the above theory is highly hypothetical for now, although I think that it could have some scientific and practical merit when designing or observing the work of such systems. In this way different large data controllers can process personal data in an automated way based on the same patterns and principles that blockchain solutions offer.

5.3 AN ANALOGY: COMMON FEATURES OF HUMAN CONSCIOUSNESS AND BLOCKCHAIN-BASED AI

Collective patterns of the functioning of human consciousness have previously been identified within the science of psychology, so I would like to introduce this before applying it to the AI and blockchain synergy. Among the representatives of the psychoanalytic school, Carl Gustav Jung pointed out in human history the identity and repetition of certain archetypic images and metaphors in each culture, which he describes as part of the "collective unconscious" of humanity. These collective psychic patterns are reflected in an individual's thought and behavior as well. Jung writes so of the collective unconscious:

> *"The collective unconscious is a part of the psyche, which owes its existence not only to personal experience, that is, we have not acquired it personally. The collective unconscious content was never conscious and therefore never acquired by the individual, but was fully inherited. While the personal unconscious consists of complexes, the collective unconscious contains archetypes. The concept of archetype expresses that there are certain forms in the psyche that can be found at all times and everywhere. The collective unconscious, like a second psychic system, is universal and impersonal in nature and is the same in everyone."*[60]

[60] Jung, C. G. (2017) *The collected works of C.G. Jung, Part 9/I.: The archetypes and the collective unconscious.* Budapest: Scolar, pp. 51-52.

In terms of classification into the philosophical schools of empirism and rationalism mentioned at the beginning of the paper (see point 2.2.), these ideas are more close to rationalism, according to which human consciousness has inherited patterns of thought and behavior.

Turning our view from the human consciousness and the collective unconscious of humanity to the examination of AI, according to Pokol, AI is becoming more and more entwined in humanity's mental layer today. The best example of this is that we are living in a society where communication is primarily based on networks of human-added and dynamically changing data flows. This phenomenon has changed the medium of communication from a physically fixed form (e.g. paper) to a state of "constant reflexive levitation" of human consciousness.[61] Kelly calls this "flowing", the fluidity of knowledge, or the phenomenon of "liquid shared intelligence" in humanity's new data-driven society.[62] The nature of communication using social media is a good example for this.

On the basis of the above, anyone in a data-driven society can add their knowledge and information to humanity's collective repository, which is an imprint of humanity's collective thinking and intelligence. AI algorithms can look for the correlations in this collective imprint of our mind and can show us similar patterns in the functioning of humanity's thinking and consciousness, including even unconscious content.

If blockchain-based data processing is compared to the human mind, we can say that individual blocks storing specific personal data may represent information stored by one's personal consciousness.

As explained above in points 5.1. and 5.2., the application of preliminary set data processing patterns in the blockchain can serve as a compliance tool to comply the data protection by design principle. Hypothetically, even the imprint of AI could be studied if automatic decisions making tools are also embedded in the blockchain.

The block in the blockchain, as a data storage unit, is thus in itself a 'tabula rasa' – using the term borrowed from empirical philosophical school –, at the moment of its birth, but the actual processing can only be carried out on the basis of data processing patterns designed by the data

[61] Pokol, B. (2018) Artificial Intelligence: The Emergence of a New Layer of Being? (AI in the Mirror of Nicolai Hartmann's Ontology). Available from: http://dx.doi.org/10.2139/ssrn.3225111 [Accessed 13 February 2021], pp. 1-2.

[62] Pokol, B. (2018) A *mesterséges intelligencia társadalma (Society of Artificial Intelligence).* Budapest: Kairosz, pp. 111-114.

controller. This is what makes these predetermined data processing patters a bit similar to collective unconscious of mankind.

In principle, the abstract rules and patterns that guarantee data protection compliance should be present when the first block is created with live personal data. Therefore, when the blockchain is being built, these patterns of legal compliance can "spread across" all blocks and all replicas of the blockchain managed by nodes. Later, the imprint of the operation of AI can be studied in the block-history. This feature could help to fine tune later data protection compliance as well.

6. SUMMARY: SYNERGY OF BLOCKCHAIN AND AI AS THE NEXT BIG PRIVACY CHALLENGE?

> *"It turned out that creating a god, as your forebears can attest, is not easy. Above all, we needed data. And he was our guy. Dempsey was rich, arrogant. He was in the right place at the right time, before the privacy laws. And his company, Incite, had all the data in the world."*[63]

We have seen above that it is possible to develop decision-making systems that can make decisions quickly and efficiently using patterns learned from personal data. Moreover, we also saw that blockchain is a data processing system that uses a distributed network structure to ensure a high level of data security and manage distributed resources efficiently. If a machine learning system uses personal data processed in a blockchain database to make decisions, it is a mix of the two systems.

According to some opinions, at first sight the development of AI and the basic operating principles of blockchain seem contradictory. This is because the efficient development of AI requires a large amount of up-to--date, high-quality data to properly teach algorithms and thus make accurate decisions.[64] As a result, only those data controllers will benefit who have the highest quality (up-to-date, accurate) data and state-of-the-art technology in their hands. Effective development today is therefore done by collecting large amount of high quality data and acquiring massive computing capability, and then focusing and centralizing it in one hand. Blockchain, on the other hand, is a technology based on the allocation of resources and data by eliminating central control, where data can be

[63] Westworld, Season 3, Episode 5.

[64] European Union Agency for Fundamental Rights (2019) op. cit., pp. 10-12.

accessed by all actors in the network.[65] However, the mixing of these controversial technologies can also lead to the democratization of the AI industry and a fair distribution of resources and data among smaller and larger players.[66] It could be also concluded that the decentralized nature of such systems may even make capable independent organizations to lawfully process data by the same data processing patterns in accordance with the GDPR's principle of data protection by design.

These ideas are mostly philosophical at the moment (and let's face it, they sound quite idealistic), but there are already AI development projects in this direction on the market, such as SingularityNET, developed to create a decentralized AI.[67]

However, as the above quote from a science fiction scenario also underlines, this technology can also be used to build institutions that are capable of fundamentally and seriously affecting human society. In the series Westworld, an AI entity with highly accurate data on the personalities and habits of all the inhabitants of Earth can foresee human fates and therefore seeks to influence lives invisibly through information society services provided to humans, effectively depriving humanity of free will. Although, according to the story, this AI runs on a centralized system, so its activity can be easily influenced or even stopped compared to a blockchain-based distributed system. A blockchain-based AI would be much more robust, yet also more transparent. Nevertheless, the impact and risks posed on those affected, i.e. humans, would be quite serious. This is why it is important to start a scientific discourse on the compliance of such systems with data protection law early on. I hope I have contributed to this dialogue through my study.

---

[65] Skalex. (2020) *AI and Blockchain: The intersection of top tech trends* [blog entry]. Available from: https://www.skalex.io/artificial-intelligence-blockchain/ [Accessed 13 February 2021].

[66] Banafa, A. (2019) *Blockchain and AI: A Perfect Match?* [blog entry]. Available from: https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/ [Accessed 13 February 2021].

[67] Member of the project team, Arif Khan, said: *"Think of blockchain as a broad horizontal layer that embraces different cultures, nations and geographical areas. Everyone can have access to this horizontal layer and interact with technology that allows people to add and work with very different sets of data. Compared to centrally managed datasets, blockchain-based databases are not controlled by any central entity."* Quotes: Wolfson, R. (2018) *Diversifying Data with Artificial Intelligence and Blockchain Technology* [press release, interview]. Available from: https://www.forbes.com/sites/rachelwolfson/2018/11/20/diversifying-data-with-artificial-intelligence-and-blockchain-technology/#407937894dad [Accessed 13 February 2021].

LIST OF REFERENCES

[1] Andrássy, G. (2008) *Philosophy and Legal Ethics.* Dialog Campus, Pécs.

[2] Article 29 Data Protection Working Party. (2017) *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (WP251rev.01). Available from: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 [Accessed: 8 February 2021].

[3] Attila Péterfalvi et. al. (2018) *Magyarázat a GDPR-ról (Interpretation of the GDPR*). Budapest: Wolters Kluwer.

[4] Bacon, J. et. al. (2017) *Blockchain Demystified*. Queen Mary School of Law Legal Studies Research Paper No. 268/2017.

[5] Banafa, A. (2019) *Blockchain and AI: A Perfect Match?* [blog entry]. Available from: https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/ [Accessed 13 February 2021].

[6] Buterin, V. (2013) *A Next-Generation Smart Contract and Decentralized Application Platform*. Available from: https://ethereum.org/en/whitepaper [Accessed 14 February 2021].

[7] Cauer, E. et. al. (2000) Life and Work of Wilhelm Cauer (1900 – 1945). *Proceedings of the Fourteenth International Symposium of Mathematical Theory of Networks and Systems (MTNS2000)*.

[8] Commission nationale de l'informatique et des libertés (CNIL) (2017). *How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence.* Available from: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf [Accessed 23 July 2021].

[9] Datatilsynet. (2018) *Artificial intelligence and privacy.* Available from: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf [Accessed 8 February 2021].

[10] European Central Bank. (2017) *How could new technology transform financial markets?* 19th April 2017. [online]. Available from: www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.en.html [Accessed 08 February 2021].

[11] European Commission. (2012) *Recommendation on preparations for the roll-out of smart metering systems (2012/148/EU) 9 March 2012*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012H0148& [Accessed: 15 December 2021].

[12] European Data Protection Board. (2020) *Guidelines on consent under Regulation (EU) 2016/679.* Available from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [Accessed 30 December 2020].

[13] European Union Agency for Fundamental Rights (2019) *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights.* Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf [Accessed 22 July 2021].

[14] Filatova, N. (2020) Smart contracts from the contract law perspective: outlining new regulative strategies, *International Journal of Law and Information Technology*, Volume 28, Issue 3, Autumn 2020. Available from: https://doi.org/10.1093/ijlit/eaaa015 [Accessed 14 February 2021].

[15] Finck, M. (2019) Blockchain and the General Data Protection Regulation. *European Parliamentary Research Service,* PE 634.445.

[16] Frankenfield, J. (2021) *Merkle Root (Cryptocurrency).* Available from: https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp [Accessed 22 December 2021].

[17] Győrfi, A. et. al. (2019) *Kriptopénz ABC (Cryptocurrency ABC).* Budapest: HVG Books.

[18] Hungarian National Authority for Data Protection and Freedom of Information. (2017) *Opinion on Blockchain Technology in the Context of Data Protection (18th July 2017)* [online]. Available from: https://naih.hu/data-protection/decisions [Accessed 08 February 2021].

[19] Infostart. (2018) *Belenéztek a fekete dobozba az ELTE kutatói (Researchers of Eötvös Lóránd University looked into the black box)* [press release]. Available from: https://infostart.hu/tudomany/2018/11/16/melytanulasi-halozatot-vizsgaltak-az-elte-kutatoi [Accessed 13 February 2021].

[20] Jung, C. G. (2017) *The collected works of C.G. Jung, Part 9/I.: The archetypes and the collective unconscious.* Budapest: Scolar.

[21] Kachorowska, M. (2019) Blockchain-based land registration: Possibilities and challenges. *Masaryk University Journal of Law and Technology*, Vol. 13. No. 2. Available from: https://doi.org/10.5817/MUJLT2019-2-8 [Accessed 13 February 2021].

[22] Kakavand, H. et. al. (2017) *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies.* Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 [Accessed 13 February 2021].

[23] Lopes, V. and Alexandre, L. A. (2019) An Overview of Blockchain Integration with Robotics and Artificial Intelligence. *Ledger Journal* Vol. 4, Supplement 1 (2019): Proceedings of the First Symposium on Blockchain and Robotics, MIT Media Lab, Cambridge, MA, 5 December 2018, USA. Available from: https://doi.org/10.5195/ledger.2019.171 [Accessed 23 July 2021].

[24] Mannan, R. et. al. (2019) GDPR and Blockchain: A Compliance Approach. *European Data Protection Law Review* 3/2019.

[25] McMurren, J. et. al. (2018) *Adressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers*. Available from: blockchan.ge/blockchange-land-registry.pdf [Accessed 13 February 2021].

[26] Pokol, B. (2018) *A mesterséges intelligencia társadalma (Society of Artificial Intelligence).* Budapest: Kairosz.

[27] Pokol, B. (2018) *Artificial Intelligence: The Emergence of a New Layer of Being? (AI in the Mirror of Nicolai Hartmann's Ontology).* Available from: http://dx.doi.org/10.2139/ssrn.3225111 [Accessed 13 February 2021].

[28] Sandner P. et. al. (2020) Convergence of Blockchain, IoT, and AI, Front. *Blockchain* 3:522600, Available from: https://doi.org/10.3389/fbloc.2020.522600 [Accessed 11. November 2021.].

[29] Sankaran, S. et. al. (2018) Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* Vienna.

[30] Schrepel, T. (2021) *Smart Contracts and the Digital Single Market Through the Lens of "Law + Technology" Approach*. European Commission. Available from: https://ssrn.com/abstract=3947174 [Accessed 26 December 2021].

[31] Skalex. (2020) *AI and Blockchain: The intersection of top tech trends* [blog entry]. Available from: https://www.skalex.io/artificial-intelligence-blockchain/ [Accessed 13 February 2021].

[32] Szabo, N. (1996) *Smart Contracts: Building Blocks for Digital Markets*. Available from: www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf [Accessed 8 February 2021].

[33] Szepesvári, C. (2005) Machine learning – a brief introduction. [lecture]. *MTA SZTAKI.* Available from: http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf [Accessed 9 February 2021].

[34] Veale, M. and Edwards, L. (2018) Clarity, surprises and further questions in the Article 29 Working Party draft guidance on automated decision making and profiling. *Computer, Law and Security Review* 34.

[35] Verbeek A. and Lundquist M. (2021) *Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy.* Available from: https://op.europa.eu/en/publication- detail/-/publication/8730fef5-315c-11ec-bd8e-01aa75ed71a1/language-en [Accessed 21 December 2021].

[36] Wolfson, R. (2018) *Diversifying Data with Artificial Intelligence and Blockchain Technology [press release, interview].* Available from: https://www.forbes.com/sites/rachelwolfson/2018/11/20/diversifying-data-with-artificial-intelligence-and-blockchain-technology/#407937894dad [Accessed 13 February 2021].

[37] Xing, B. and Marwala, T. (2018) *The Synergy of Blockchain and Artificial Intelligence.* Available from: http://dx.doi.org/10.2139/ssrn.3225357 [Accessed 13 February 2021].