EU Business Law and Digital Revolution

Pre-print manuscript

EU Business Law and Digital Revolution

– Selected Studies from New Fields of Technology

Széchenyi István University
Deák Ferenc Faculty of Law and Political Sciences
Department of International and European Law
2019

Editors:
Judit Glavanits
Balázs Horváthy
László Knapp

The manuscript has been reviewed by László Milassin.

ISBN 978-615-5837-64-7 (Print)
ISBN 978-615-5837-65-4 (PDF)

This book has been published within the research stream of "Jean Monnet Module on EU Business Law" (EUBLAW) funded by the Erasmus+ Programme of European Union.
Győr, 2019

Jean Monnet Module on
EU BUSINESS LAW
2016 – 2019

Co-funded by the
Erasmus+ Programme
of the European Union

Published by Széchenyi István University –
Deák Ferenc Faculty of Law and Political Sciences –
Department of International and European Law
(H-9026 Győr, Áldozat u. 12.)
Tel.:+36/96/503-478
Fax: +36/96/503-472
Web: nejt.sze.hu

Content

Content 5

Foreword 7

I. Artificial Intelligence: legal implications

Knight Rider's Brothers Coming Soon – What About Their Legal Situation? 11
(*Gábor Kertész*)

Artificial Intelligence and Bid Rigging 29
(*Mária T. Patakyová*)

Fear the Robots? – Attitudes from the Supply Chain 43
(*István Pesti-Farkas – Zoltán Szegedi*)

AI Risk Assessment Tools: The Trojan Horse of the Criminal Justice System 51
(*Laura Stănilă*)

II. Cryptocurrencies

Central Bank Issued Digital Currencies: is it a Solution or a Problem? 71
(*Zsolt Bujtár*)

Fluidity of Term of Cryptocurrency – A Challenge for Regulators 89
(*Sonja Bunčić – Alpar Lošonc – Andrea Ivanišević*)

Virtual Currencies – Legal Challenges 113
(*Zsolt Halász*)

The Classification of Virtual Currencies Related to Blockchains 133
(*Péter Bálint Király*)

Cryptocurrencies: A Theoretical Approach 149
(*Andrea Labancz*)

III. Business and digitalization

Adoption of ICT in Higher education: Readiness of University Students in Rural India 171
(*Neera Chopra*)

Electronic Commerce in Gaming Industry. European Perspective on the Legal Regulations of In-game Virtual Transactions..... 193
(*Olena Demchenko*)

Smart Cities, Iot and Blockchain: The Importance of Oracles ... 209
(*Judit Glavanits*)

Autonomous Vehicles – Challenges for EU Private International Law 233
(*Balázs Horváthy*)

Annex – The Centre for European Studies (CES) at the Széchenyi István University 255

Foreword

In 2017 the Centre for European Studies (CES) of Faculty of Law and Political Sciences of the Széchenyi István University launched the conference series '*EU Business Law Forum'* with the aim to establish a regular event, which reflects on topical issues of EU business law and explores the related contemporary challenges in their legal, political, economic and social reality.

The 2nd EU Business Law Forum *"EU Business Law through the lens of Digital Revolution"* held between 13–14 June 2019, was devoted to discuss the implications of the current technological revolution on the business environment in the European Union, particularly on the EU business law regulation. The Forum identified the recent challenges that the EU business actors are facing as a result of the digitalization and posed the question, whether – analogically to the concept of 'Industry 4.0' – a process of a 'Law 4.0' is expected to become tangible in the EU business law regulation, responding adequately the challenges arising from the new disruptive technologies.

This book offers an insight into the main focus areas of the conference. The first chapter (*I. Artificial Intelligence: legal implications*) reflects on the growing importance of using artificial intelligence and the role of the legal regulation. The articles pose questions form general as well as specific perspectives and illustrates the legal problems of the artificial intelligence by varieties of topics, from the public procurements to the supply chains. The second chapter collects the papers that are focusing on the new instruments of exchange (*II. Cryptocurrencies*). The chapter lays down the conceptual basis of cryptocurrencies and examines the legal and regulatory challenges arising from the current use and the probable future prevalence of the virtual currencies. The third chapter of the book pays attention to emerging fields of regulations (*III. Business and digitalization*).

The papers examine the adoption of technological innovations in higher education, e-commerce related aspects of computer games, legal challenges of smart contracts and autonomous vehicles.

The Forum was a part of the 'Jean Monnet Module on EU Business Law' (EUBLAW) project funded by the European Commission's Erasmus+ Programme in the Period of 2016 – 2019, and this year, the CES organized the event in cooperation with the SmartLaw Research Group.

Editors
Győr, December 2019

I. Artificial Intelligence: legal implications

Knight Rider's Brothers Coming Soon – What About Their Legal Situation?

Gábor Kertész*

Abstract: Nowadays, we are confronted more and more times with the issues of artificial intelligence and (partly or completely) self-driving vehicles. How does this technical development change our daily lives? What can "Law" do with these? In the analysis I am looking for the answer how these technical novelties can fit into the structure and logic of the legal system. During this process I use examples of history and legal history, other social sciences and modern business logic as well.

Keywords: artificial Intelligence, self-driving cars, responsibility for damages

1. Introduction

In the 1990s, television channels broadcasted the Knight Rider action film in a huge number of countries around the world, in which one of the main characters was a self-driving car. That time it existed only at the level of dreams and on the design tables of engineers, today it is reality in some parts of the world.

1.1. A bit of „layman philosphy"

Our long-standing expectation towards machines to work perfectly, flawlessly. In the contrary our recurring experience is that "nothing is perfect" "what may go wrong will go wrong" and we have to admit that a thing without any errors has never been made by a non-perfect person. From this point of view, we can ask how many % of the errors are accepted in practice naming the thing "perfect" or rather appropriate.

The concept of damage appears already in the earliest legal systems. The concept clarified in the old Roman law is still perfectly applicable today, according to which the damage has two parts: the real damage (*dannum emergens*) and the loss of profit (*lucrum cessans*). Based on

* College professor, International Business School (Budapest).

these, it is a question of argumentation to determine whose (active or passive) behavior caused the damage and who bears responsibility for the damage. It is usually a judicial procedural task not to allow the evidence procedure to sink into the infinite marsh of the principle of *conditio sine qua non*.

2. Historical examples

2.1. Legal instruments nowadays that come from legal history

These legal instruments of responsibility have been created in the history of law during the technical development to solve the current problem. Man first tamed / domesticated animals that typically followed his instructions, but sometimes did not or not well executed the instruction and caused damage. The issue of liability for such damages caused by animals has been established long ago, and its structure has not changed since the first civilizations, and our act uses their logic still today.[1] Also, since the earliest settled civilizations where built environment has been built, the question of damage caused by objects falling from buildings[2] is known. Although the material and design of our buildings have undergone many changes over the past millennia, the handling of damages by objects falling from the buildings has not changed much over the past two thousand years. The next form of responsibility was developed due to another historical step that was the industrial revolution. The concept and liability of dangerous operations[3] is approached by the structure that was formed at that time, although nowadays many of these types of "operations" operate on a daily basis, and only the detailed rules for the new types are added to the centuries-old structure. The last type of liability (although it can still be argued that this is not yet clear, but still in the process of being developed) is product liability[4], where the link is created between the manufacturer and the end

[1] Liability for the damages caused by animals Ptk. 6.:562-563. §. Here and thereafter, I refer to certain provisions of the Hungarian Civil Code (Ptk.), which has the same content in civil law in all the legal systems of the world.

[2] Liablity for building damages Ptk. 6.:560-561. §.

[3] Liability for dangerous operations Ptk. 6.:535-539. §.

[4] Product liability Ptk. 6.:550-559. §.

user of the product by omitting the intermediate elements of the causal chain.

As a continental lawyer I looked for similar cases for autonomous, self-driving vehicles. One of the "precedents" - using several multiple quotation marks - is the case of animal damages[5]. In this case an animal with independent autonomous animal intelligence causes damage and it is a partial question if the owner "led" the animal, or is made itself independent or uncontrollable. The other case that could be a "precedent" is the liability of the legal entity, where the legal person that caused the damage, will be liable for the damage and the legal entity will be obliged by the court to pay the compensation for the damage.

With legal logic and expert arguments on a case-by-case basis, it is possible to determine in which proportion and percentage the potential responsible people (responsible groups) listed and analyzed above are responsible for the damage. The traditional market logic provides insurance as a solution to a potential threat, where we can atomize the actual damage between the members of the risk community.

Another possible answer of business logic is to burden the damage to the one who caused it. Here the legal logic says today that to oblige a damage-causing truly self-driving vehicle to indemnify the damage, it should be a legal entity. Not going into the solutions of ancient - not Roman - and medieval rights that have passed the ownership of the damage-causing animal, or the harmed received temporary use on the animal, in case of self-driving cars the similar solution is possible, as it is a fact that the damage-causing thing has a value for use and it is able to produce it regularly.

2.2. Philip IV. (the Fair)

The next example is about a minor change made by the legislator that made a huge change in the historical perspective and that fundamentally influences national identity. Philip the Fair, king of France ordered in 1308 that in a case between non-barons, the court established at that time and permanently operating at the Royal Palace in Paris should make a final decision either in direct action or in appeal against a provincial judgment. This court used the local language around Paris and its code of conduct

[5] Ptk. 6:562.563. §

made it clear to accept only contracts and actions written in the language of the court[6]. From the early Middle Ages in today's France, the provinces with individual feudal autonomy spoke their own local language[7]. As a result of this law, in just a few decades, the language of the court became known as a written language in every corner of the Kingdom of France, which we now know as a French language, as it was in everyone's interest to write all the contracts in that language. Nowadays, French is an important element of French national identity.

This is a good example of the fact that standardization of the rules for the use of certain elements of Artificial Intelligence (e.g. self-driving cars) will be significant for all members of society and will have a social organizing and forming effect in the long run.

3. Who can be liable if Knight Rider makes an accident?

Let us shortly list the different human beings who have any connection with Knight Rider's birth.

3.1. Possible liable people

3.1.1. Driver

This is the only member of the coming list, where - according to the current Hungarian legal environment - only one natural person can be a subject. Until now, the liability of the driver was an evidence in the case of damages caused by man-, animal- or machine powered vehicles. Nowadays there are vehicles that are not driven by humans, but are driven by the intelligent / autonomous vehicle itself in self-driving, however in the Union they drive only on test fields, not in real traffic. After a broad social debate involving the whole human civilization, it can be agreed if the natural people in self-driving vehicles should, and if so at what level, control the proper / accident-free operation of the vehicle. Currently, although we have already met a few legal cases, where the responsibility of the driver has been established on the basis of traditional logic, neither

[6] Pál Horváth, István Kajtár, Lászlóné Nagy, T. Mihály Révész, István Stipta and János Zlinszky, *Általános jogtörténet I.* (Nemzeti Tankönyvkiadó 1994) 64.

[7] This was the language of the certain Gaul tribe from which the people of the province originate.

the public opinion nor the legislator has conducted this increasingly necessary debate yet. If the decision is made, it can be translated then into a known form of liability. According to the current Hungarian rules, if the vehicle is in motion, one person must be in the driving position continuously[8]. The Hungarian practice has not yet faced a case when the vehicle was self-driven with an empty driver seat causing an accident / damage. However, with the development of technology the question has to be answered soon whether the person who switches the vehicle into self-driving mode is a driver according to the Road Traffic Code? Does this person stay a driver after leaving the vehicle, which continues the way in self-driving mode? With traditional legal deduction the question can be replied in a conventional way. In this case, the question is modified to the following: does it worth to invest in the development / acquisition of such a vehicle, if my responsibility for a self-driving vehicle is the same as if I were actually driving it? Or how worthy it is for me if I have possibility to do other activity(s) besides controlling the vehicle during sitting in the driver's seat?

3.1.2. Owner

The Road Traffic Code basically lays down rules for the traffic participants: the driver and the passenger, and the owner appears only once in the text[9], but in the meantime the owner is recorded separately in the traffic license. We have been treating it for thousands of years as an evidence that the owner is responsible for the damage caused by his property.[10] It is important to recall here for a moment the analogy that the tutelary is responsible for the damage caused by the unpunishable person.[11]

3.1.3. Retailer, Wholesaler, Importer

[8] Road Traffic Code (KRESZ) 4. §.
[9] Road Traffic Code (KRESZ) 59. § (3) subpar.
[10] See e.g. footnote no 2, 3, 4.
[11] Liability for damages caused by unpunishable person Ptk. 6:544-547. §.

At this point, we arrived at to the actors of the sales chain, calling the person[12] - in practice typically a legal person - a retailer who sold the vehicle to the owner; the other players are working on the basis of traditional trade contracts, their responsibilities are governed by the contracts, the relevant customs and the practice of the judiciary and arbitration court.

3.1.4. Tester team

Here, on the one hand, it is the task and responsibility of the team to perform all the necessary tests thoroughly and professionally and on the other hand to ensure that all relevant tests are performed. Although this team typically consists of engineers, they have to keep in mind that they have to test the vehicle in every theoretically possible situation and check how it behaves in each case. It is often told about us as lawyers that we are writing novel-length contracts as 'graphomans' in which we try to get prepared for every single theoretically imaginable risk factor. The test team has a similar task to examine how the vehicle responds in a self-driven mode to the variety of all theoretically possible situations. For the test team only the collective responsibility can be imagined, since the outstanding and indispensable contribution of a team member is theoretically conceivable, but apart from such extreme situations, the contribution of all members of the team is equally important for the proper performance of the test and the evaluation of the result. Although they are not members of the testing team, but the decision-makers of the enterprise also have a responsibility here, as the management decides based on the results of the tests, with engineer, lawyer and economist support if the vehicle is ready to be put on the market / in traffic or further development is needed.

3.1.5. Szoftverfejlesztő csapat Softver-developer team

This team develops the software (system) that ensures the vehicle's self-driving ability. Nowadays, developers generally “teach” the systems in a way that it faces decision-making situations continuously, and it achieves a better percentage of success due to this “learning”. The other,

[12] I examine only the sales of new vehicles. The sales of used vehicles is out of scope of the examination.

nowadays in minority applied solution is to program the "right / good / desirable" solution and the system has to avoid the rest. The responsibility of the developers is unavoidable for both methods. In the first method the responsibility originates in the examples that were the base for teaching the system. It can happen that even though the sample consists of a large number of elements, there can be cases that are out of the model and the machine will not recognize them and it will not be able to handle them well. In the second method, the more detailed description of the good solution is important, so that the machine can handle the situation that actually arises, even if it is new, but similar to a learned rule. At this point, the question of the need for ethics arises. If in a given situation only bad decisions can be made and non-decision is also a bad decision, which wrong decision should be made by the Artificial Intelligence that was taught and built in the system?

A comprehensive research project was launched in 2016 with 40 million people worldwide, related to the artificial intelligence-driven cars being developed nowadays. Researchers were looking for an answer to what people say: if there is no way to avoid an accident, who should hit the car? The answers outline a world-wide view of what we are protecting more and what less. The results of the research have been published only half a year ago[13]. The article first states that it cannot be considered worldwide statistically representative because of the limited possibilities of sampling, but the data collected show that children are more likely to be saved than adults, but this is only a global average statistical result, because the range of bad decisions differ from country to country and even more from culture to culture. The results of the world average are not the same as the results of the regions and metropolises that are the most multicultural according to sociologists. So according to the data, people in different cultures of the world set different order of importance, or approach the question from the other side, a different order is set in the list of other people and objects to be sacrificed. So, if there are such significant sequencing differences in case of people from different parts or different cultures of the world, in which order to protect the different values in an emergency, then Artificial Intelligence will also not be able to

[13] Edmond Awad, Sohan Dsouza, Richard Kim, Jonathan Schulz, Joseph Henrich, Azim Shariff, Jean-François Bonnefon and Iyad Rahwan, 'The Moral Machine experiment' (Nature, 24 October 2018).

decide according to a generally accepted sequence, although such situations relatively often occur during traffic.

In this case, the question arises which culture's prioritization will be the base for the self-driving vehicles choice, i.e. which sequence was programmed/taught by the programming team. Here, group dynamics and hierarchical relationships within the group as well within the organization can also influence the sequence they teach, along with the cultural patterns of the team members and other individuals involved. I.e. if the development team is culturally homogeneous and whether the final decision-making management has the same, homogeneous cultural background. For most of these companies, we cannot say yes to this question with a calm heart. This results in the following: there is a significant likelihood that the sequence of priority will be determined differently by not only the vehicle types produced by the different manufacturers, but also by the same brand and type of self-driving cars, if they are produced in different plants of the world far away from each other, if Artificial Intelligence is made independently in the plant, rather than installing a centrally-produced system in vehicles manufactured in all factories around the world. The issue is about the choice of victim[14] in an inevitable situation of a self-driven vehicle programmed under the rules of other cultures. In my opinion this issue can be settled satisfactorily through an agreement resulting from a consultancy with the presence of the whole world, or if the producers mutate the vehicles into the different cultural regions where they are sold. It is not primarily a business law issue, but a fundamental rights issue if it is allowed to the owner/driver to download versions of other cultures; either because he disagrees with the culture of his place of residence and feels another his own, or because he is planning to go to the territory of this culture - though the latter can be automatically solved by the service that if the vehicle crosses the "cultural boundary" according to its GPS coordinates, the system downloads the version that is valid in that area.

3.1.6. Planner team

This is a team consisting of mostly engineers who design the "hardware" of the vehicle. In addition to the fault possibilities of

[14] E.g. the choices were different when the vehicle hits the old person or the child in order to save the other one – see same as footnote no 13.

conventional vehicle design, only one new risk factor appears here. It is a well-known experience in conventional vehicle driving that there are "dead spaces" in case of all vehicles depending on the vehicle's size, which are not visible to the driver. Their magnitude cannot be completely removed, only reduced with the rear-view mirror system. In case of self-driving vehicles, however, the expectation is that the machine should see everything in real time, simultaneously and drive itself accordingly. That's why the design team here, beyond the usual design responsibilities of traditional vehicle design, has to meet „only" one new requirement. On the vehicle the environment sensors must be positioned so that they can continuously see all objects in real time within the current speed braking distance that would presents a risk of accident in case of going without change. (Of course, the danger of a new object that might come out of the cover of another object is excluded here.) If the design really reduced the size of "dead spaces" for self-guiding sensors to 0%, the design team does not have any more responsibilities than the ones coming from traditional design responsibilities. The current traffic situation was detected by the sensors that transmitted it to the software, which made the decision in self-driving mode, which is the result of the work of the development team[15].

3.1.7. Controller team

Modern states usually have a body that controls various activities carried out by economic actors. The depth of control that this body performs varies from body to body and from country to country. If a causal link can be established between the authorization procedure of the authority and the damage caused, the determination of damage caused by administrative law may arise if it was not possible to avert the damage by ordinary legal remedy or in administrative juridical action[16]. The theoretical possibility of this in the examined issue arises only if such an error originating in the type of the self-driving vehicle, which has not been recognized either by the licensing authority or the manufacturer's designer, software developer and test team previously.

[15] See footnotes no 13 and 14.
[16] Ptk. 6: 548. §.

3.1.8. Legislator

Legal acts created by the legislator are applied by legal entities and by the executive and judiciary branches. And it is a century-old, if not a millennium-old fact, for which we can find more and more examples nowadays that it is possible to legislate only such situations that already occurred, or they could be predicted with significant possibility. The new life situations that have arisen after the legislation have typically appeared as a legal loophole in continental law systems, and in the Anglo-Saxon systems precedents are sought. From a legal point of view, the “legislator's silence” - if no law was created on the certain situation - cannot be interpreted as a damaging fault. However, economic actors can perceive it as a damaging fault according to the logic of the economy, of the business and if the market. The question that arises here is whether the legislator has created the legal system so that it is able to deal with the problem of damage caused by a self-driving vehicle, and whether this solution is appropriate for society (for voters?).

3.2. How can Knight Rider be liable?

According to the basic division in law, there are legal subjects and legal objects. There are no third and temporary categories. We neglect to discuss the historical development of the general, unconditional and equal legal subject people have. We only mention the last step in the development of legal entities, the second group of legal subjects known today: "The legal personality of a legal person extends to all rights and obligations that, by their very nature, may not only be related to a human being"[17], i.e. the legal personality of the legal person is not bound to a purpose, but it is general. It is not a matter of jurisdiction, but a matter of legislation which listed actors and in which extent are made liable for the damages caused by the self-driving vehicle. It is already the task of political science to examine political programs, political marketing, and legal lobbying of the interested companies.

Taking the two premises into consideration that the self-driving vehicle is capable of making autonomous decisions - respecting the rules of social cohabitation - and is capable to generate financial value continuously, the business logic raises the question in a right way why this vehicle cannot

[17] Ptk. 3:1. § (2) subpar.

be an actor in business life on its own? As besides people - nowadays mainly in the international business community, instead of people – it is worldwide an accepted evidence by everyone and everywhere that "legal constructions" named legal entities have legal subject, independent from the fact that no one has seen a legal entity, only a person representing it, its logo, or its headquarters. However, the self-driving vehicle is a tangible physical reality.

Since the concept of a legal person appeared in legal history till the present, there is clear evidence that non-human private entities ultimately have a human owner. Nowadays, a new concept has emerged on the periphery of the legal subjects, which is the "actual beneficial owner" who increases its assets with the values produced by the examined legal entity, or has the right to dispose of these assets either directly or through mandatory instructions given to the participants in the chain[18]. Not going into details in the psychological, corporate, and social sociological question of what group dynamics each company (regardless of its legal form) has; we can say that the purpose of the company (the legal entity in question) is to live / operate further. As an analogy to this approach, we can assume that the autonomous, self-driving vehicles are also aimed for further operation; however, this hypothesis gives the software development, testing, and control teams an important task. The mentioned research looked for a reply about who the vehicle would rather hit[19]. For a human driver, it is an existing option, for which there are some famous examples, that the person sacrifices his own life, and with this, saving many. With the sensors of the vehicle's seats, on the base of the weight of each passenger, the vehicle "knows"[20] how many adults and how many children are traveling in it, and even through the implementation of this data and the decision of the software development

[18] About the concepts „beneficial owner" and „actual beneficial owner" see the different conventions about avoiding double taxation and 7. point of 7. App of the Hungarian citizens income tax act.

[19] Awad et al. (n 13)

[20] Not going into details about the results of Awad et. al. (n 13), according to which the general cultural reply to this in Europe is that the driver puts suitcases on each seat with a weight equal to a child's weight and fastens the seatbelts. With this the Artificial Intelligence counts with one adult and more children and its own safety on the one hand, and takes into consideration the safety of the person/people involved in a possible accident on the other hand.

team it can save endangered people in a “self-sacrificing way” with a "death manoeuvre" sacrificing itself and its passengers.

4. Let me introduce Knight Rider

In case of Artificial Intelligence built into the self-driving vehicle from the legal aspect of responsibility it is important to refer to the “deep learning”[21] technique used to “teach” these vehicles. With this "learning technique" the Artificial Intelligence does not "try through" all possible combinations during problem solving, but after the first recognized (or thought to be recognized) model mark, it searches for the next one and then goes on step by step and defines the created pattern as a test result. It is up to the development team to decide how strictly and with how much data they teach the vehicle, or in which extent they let it learn independently. After a certain level of knowledge the system can "learn" and acquire relevant knowledge and information without the help of human or other Artificial Intelligence, to improve its operational efficiency[22]. At this level of learning we can already say that Artificial Intelligence is a "black box", because it is not possible to derive and reconstruct all details required for the judgment of a certain important decision it made. Because the example(s) used to make the decision in question was not “taught” by man, but the vehicle has made a decision on the base of the examples taught and examples it created and solved alone with mechanical logic, and this may result in causing damage. During the deep learning self-study after the thoroughly taught knowledge of the Artificial Intelligence, no one can be made logically or legally responsible for "teaching" the example that causes the damage in the certain case, so the owner of the self-driving vehicle will be responsible for the damage even if the owner was not in the vehicle.

In the previous section we dealt with a lot of potential responsible entities. There are many hypothetical emergencies similar to the example, cited in footnote 22 above, the solution of which raises a moral and ethical issue if not a self-driving vehicle, but a human being is involved in the certain situation. Therefore, in my opinion, the software development

[21] Y. Bengio, A. Courville and P. Vincent, ’Representation Learning: A Review and New Perspectives’ (2013) 35 (8) IEEE Transactions on Pattern Analysis and Machine Intelligence 1798–1828

[22] Yoshua Bengio, Yann LeCun and Geoffrey Hinton, ‘Deep Learning’ (2015) (521) Nature 436–444.

team must work closely with lawyers and ethics professionals so that autonomous self-driving vehicle will be able to provide answers that correspond to the legal and general ethical principle of the certain culture in case of emergencies. Accepting and acknowledging the fact that different cultures on Earth differently set the sequence of importance of the values to be protected, it seems logical to harmonize these sequences by convening an international meeting with politicians, ethics and legal professionals, which results in the code of ethics that is to be programmed in all vehicles capable for self-driving as a ROM[23] memory. Such a "moral code" burned in all self-driving vehicles at world level raises the question of the autonomy and "free will" of all people, since the computer code of ethics, written on the base of international consensus, will depart from the moral opinions of individual people, as it is the consensual opinion of the ethical opinions currently existing in the world. It is no longer a matter of law, but of politics, how or how to transform the general moral code of mankind in the ranking of values to be protected by applying social engineering. This would undoubtedly raise fundamental rights issues in all states, as it raises the possible risk of personal and / or community identity transformation. There are such examples in history; they are often referred to as a deterrent.

Till now we have seen some important historical examples how a legal object become a legal entity (not going into the evident solution in continental law as to exemplifying with "old Romans", the way of creating a legal entity with the regulation of "emancipation"). Looking at the legal history - and the history of mankind – and searching for the answer to the question why a legal subject has been transferred to legal entities, we can find three different answers, three reasons. The first is the "pro bono" reason, which was typically the owner's own sovereign decision, and after it became widespread, it was made by law general[24]. The second is a typically a violent step, coming from the one-sided decision of the certain object, when it takes out itself from the real power of the owner. In history these are called "slavery insurrection". Their goal - becoming a legal entity

[23] ROM: Read-Only Memory. It is part of the memory of an electronic system the contents of which are read-only, non-erasable and non-rewritable. Data are physically recorded so that they are "remembered" even when disconnected from power, and physical erasure of data results in physical damage of the device.

[24] Not going into details about the social-psychological and sociological consequences of the change of the legal term „instrument vocale" to „servilis persona" in the early Middle Ages.

– was reached in a negligible percentage in a global historical context, but the economy of the given society or of a narrower community was affected in all cases negatively, but to varying degrees. While the previous two reasons are human, the third reason is economic.

5. A potential interest for Knight Rider's legal identity

In a group of legal entities – today we call them capital owners today – appeared the need to separate their entrepreneurial and private assets. The main reason for this was to avoid that in case of bankruptcy of the company the owner's personal property would be lost, too. This is how through the complete separation of business assets from private assets, a new legal subject type was created: the legal entity that has an owner, but its legal subjectness is separate[25], and its existence has a purpose[26]. In this context, it is important to remember that the legal entity must have a purpose according to law, not only in the Hungarian legal system, which obligation can be fulfilled by the recording of an activity according to TEÁOR (Hungarian statistic register of economic activities) in the founding document. But the legal capacity of the legal entity covers all rights, legal protection and obligations that are due to their character inherently bound to human people[27].

Nowadays, the new issue, the new challenge is providing a reason for giving legal subjectness to the self-driving vehicle, which can be obviously only an economic reason. Based on current trends, these vehicles, especially because of the control software, will be so expensive that they can expect top or premium pricing. This excludes the wide range of private ownership of vehicles, which is general in today's culture everywhere. In legal practice "shared use rights[28]" is a known legal institution. If we convert this existing legal institution so that the subject of it (on which it is possible to gain shared use rights) is a self-driving vehicle, for which the usage fee can be paid to a particular bank account, and from the balance of this account the vehicle's fuel and service costs, is compulsory insurance and the compensation of the possible caused damages can be

[25] See: Actio Pauliana in the Roman Law.

[26] Ptk. 3:5. § c) point I. turn.

[27] Ptk. 3:1.§ (2) – (3) subpar.

[28] In the Anglo-Saxon legal literature it is known under the concept „timeshare" or „vacation ownership".

paid, we come to a "target asset". The concept of "target assets" has been known in legal literature for a long time, without examining the types of public target assets and private law is more familiar with the concept in connection with foundations. The essence of this has not changed since the creation of the concept: the assets of the foundation can be used only for the permanent purpose[29] defined in the founding record. And it can be a "permanent purpose" that the self-driving vehicle should work. The provision of the above-mentioned bank account and its handling can be provided by a computer algorithm nowadays. Such an algorithm can be installed in the vehicle without any problems, so the self-driving vehicle can "dispose" of the shared use by using this algorithm, or from other point of view it can cover its costs of operation and maintenance and any possible damages from these revenues coming from the charges of passengers for transport services.

From this point on, however, as there is a target asset[30] with significant value, we can determine as a permanent goal the maintenance of the continuous operation of the vehicle and the compensation of the damages caused. To achieve these goals, there is an algorithm that does not require direct human help to operate the target asset. The decision to classify this complex legal object as a legal entity can be made after a broad social debate. The question from the business side appears if it is finally worthy being the owner and thus being responsible for any possible damages the self-driving vehicle as an object causes? If the answer is yes, the liability options known in the legal system can be used to manage disputes, and jurists have only "law enforcement" responsibilities. If the answer is no, then jurists should collaborate with other social scientists, engineers and mainly software development programmers in order to find the right answer.

6. Conclusion

I investigated self-driving vehicles – for a more plastic presentation with the use of the title of an old film series about a knight, Knight Rider – to find out, which scenario would be realistic: will it become a robber knight, a Grail Knight, or a simple ordinary knight? During our investigation

[29] Ptk. 3:378.§ 3:382. § 3: 384. §.

[30] In accounting terms the self-driving car is tangible asset, and the bank account it controls/handels is a current asset.

we have found that there is a good chance that after the "page" training, the society will have the self-driving car as an efficient, labor-intensive "gear" in the system. However, to become a Grail Knight, the training must be developed globally, but any mistake during the development of this system can result in making it a robber knight. From the example of Philip the Fair, we have seen that changing central laws to simplify bureaucracy can, in the long run, strengthen community identity as a side effect. In the case of self-driving cars, we see that sooner or later, it will be necessary to establish uniform rules all around the world so that in emergency situations there will be no random choices between values and lives. Today, we cannot yet say how such a quasi-ethical system that should be programmed into self-driving cars for such emergency situations will effect the ethical rules of people and of different societies.

References

- Awad, Edmond; Dsouza, Sohan; Kim, Richard; Schulz, Jonathan; Henrich, Joseph; Shariff, Azim; Bonnefon, Jean-François and Rahwan, Iyad, 'The Moral Machine experiment' (Nature, 24 October 2018)
- Bengio, Y.; Courville, A. and Vincent, P., 'Representation Learning: A Review and New Perspectives' (2013) 35 (8) IEEE Transactions on Pattern Analysis and Machine Intelligence
- Bengio, Yoshua; LeCun, Yann and Hinton, Geoffrey, 'Deep Learning' (2015) (521) Nature
- Horváth, Pál; Kajtár, István; Nagy, Lászlóné; Révész, T. Mihály; Stipta, István and Zlinszky, István, *Általános jogtörténet I.* (Nemzeti Tankönyvkiadó 1994)

Short biography of the author

Gábor Kertész PhD received degree in law at Pázmány Péter Catholic University at the Faculty of Law Sciences. He worked as a financial investigator between 2002 and 2006 and I have investigated cases about tax evasion and bankruptcy crime. Between 2006 and 2008 he worked as solicitor and from 2008 till 2018 as lawyer. Besides this he educated at the business law department of the Budapest College of Management. In 2012 he received a PhD degree. In 2013 he was nominated college professor. Now – since the fusion of the institutions – he educates at the

International Business School in Budapest. He is a member of the editorial board of the Hungarian Bioethical Review and of the Economics World.

Artificial Intelligence and Bid Rigging

Mária T. Patakyová *

Abstract: A special attention of competition authorities has lately been attracted by one particular type of collusive practice – bid rigging. No wonder, it has a significant effect on both proper functioning of competition and proper outcome of the procurement procedure. Instead of competing, undertakings collude among each other; and instead of the best bid, the public procurement procedure is won by a bid coming out of collusion. Within such state of matters, this paper aims to elaborate on the role of artificial intelligence in bid rigging. It is claimed that artificial intelligence is often used by undertakings which may lead to difficulties in identification and prosecution of infringements of Article 101 TFEU. What are the particular issues brought by the use of artificial intelligence? Are there any positive effects, or does it make the whole enforcement more onerous? These are the questions to be discussed by this paper.

Keywords: competition law, horizontal agreements, 101 TFEU, bid rigging, artificial intelligence, algorithm

1. Introduction

Technology has a tremendous impact on a way how business is done. Human beings are being replaced by algorithms and artificial intelligence. This may lead to higher efficiency and, consequently, to lower prices for products and services. On the other hand, it creates a space for easier commitment of prohibited activities.

One of these prohibited activities is discussed in this paper. Horizontal agreements represent the infringement of competition law which is, arguably, punished the most. There are good reasons for that. Cartels jeopardise the very essence of the competition, the fact that competitors *compete*. This leads to poorer quality of the products and services, often accompanied by an increase of prices. On the top of that, cartelist usually

This paper was supported from a Grant project of "Agentúra na podporu výskumu a vývoja v rámci projektu č. APVV-17-0641 "Zefektívnenie právnej úpravy verejného obstarávania a jej aplikácie v kontexte práva Európskej únie"."

* Assistant professor, Comenius University in Bratislava, Faculty of Law, Institute of European Law, maria.patakyova2@flaw.uniba.sk.

hide well the existence of the cartel, which complicates the enforcement to a great extent.

In particular, this paper zooms in on horizontal agreements in tendering procedures. Bid rigging is even more deplorable as it ruins the efficient spending of public money. Therefore, not only buyers of the products produced by cartelists suffer from poorer quality and higher price, but all taxpayers suffer, as spending of tax they pay is not used in accordance with the "*value for money*" principle.

This paper aims to identify which issues are brought by use of algorithms and artificial intelligence in relation to bid rigging. In particular, the paper zooms in on methods of competition law enforcement using new technologies, especially regarding public procurement. Apart from that, the employment of algorithms is analysed from the perspective of how it can mitigate collusive behaviour.

In order to discuss these issues, the paper is organised as follows. In the beginning, bid rigging as a form of horizontal agreement is briefly presented from substantive and procedural point of view. Subsequently, the employment of algorithms and artificial intelligence is discussed; firstly, as an assistant for investigation of cartels and, secondly, as an assistant for collusion. Concluding remarks are presented in the conclusion.

2. Bid rigging

Article 101 para. 1 TFEU prohibits agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market. Pursuant to this wording, there is a difference between agreements and concerted practices. Agreements are understood as a concurrence of wills between at least two parties. The form of the agreement is irrelevant so long as it constitutes the faithful expression of the parties' intention.[1]

There are cases where the agreement is not reached by the parties, but the situation on the market is not natural. Concerted practices should

[1] Judgment of 6 January 2004, *BAI and Commission v Bayer*, C-2/01 P, EU:C:2004:2, para 97.

capture such instances, where the parties cooperate on the market.[2] The concerted practice is characterised by the fact that it cannot be understood as a natural following of other party's behaviour on the market. It is therefore clear that the parties are coordinated.[3]

It is possible that a prohibited agreement (in a broader sense) is exempted by a general block exemption regulation or by Article 101 para. 3 TFEU. This is also applicable (at least in theory) to restrictions by object. However, the burden of proof lies on the undertaking who wishes to benefit from the exemption.[4]

Furthermore, this type of anti-competitive practice is also prohibited by national law. Taking Slovak law under scrutiny, Section 4 of Act No. 136/2001 Coll. on protection of competition, as amended, prohibits anti-competitive agreements as well. The Slovak regulation is *de iure* and *de facto* very similar to the EU regulation.[5]

As it flows from the wording of Article 101 para 1, agreements can have two forms – by object and by effect. The prohibition of by object agreement is rather self-explanatory. It means that the agreement has as its very purpose the prevention, restriction or distortion of competition. In general, by object agreements captures horizontal agreements: "*to fix price, to exchange information that reduces uncertainty about future behaviour, to share markets, to limit output, including the removal of excess capacity, to limit sales, for collective exclusive dealing*".[6] Bid rigging is also a type of by object agreement.[7]

The other type of agreements, by effect agreements, requires rather detailed analysis of the agreement's effects on the market. Although a presentation of certain economic thoughts is required in a decision fining

[2] Damian Chalmers, Gareth Davies and Giorgio Monti, *European Union Law* (3rd edn, Cambridge University Press 2014) 1008.

[3] Peter Demčák, 'Dohody obmedzujúce súťaž' (Conference Efektívnosť právnej úpravy ochrany hospodárskej súťaže – návrhy de lege ferenda, Bratislave, 2017) 24.

[4] Cyril Ritter, 'Joint tendering under EU Competition Law' (2017) < http://ssrn.com/abstract=2909572> accessed 14 August 2019, 16.

[5] Mária Patakyová, 'Vplyv Európskej únie na legislatívu Slovenskej republiky v oblasti hospodárskej súťaže' (Conference Míľniky práva v stredoeurópskom priestore, Častá-Papiernička, 2015) 124.

[6] Richard Whish and David Bailey, *Competition Law* (7th edn, Oxford University Press 2012) 124.

[7] Katarína Kalesná, 'Tendrové kartely a ich špecifiká' (Conference Aktuálne otázky súťažného práva v Európskej únii a na Slovensku, Bratislave, 2015) 23, 30.

by object agreement too, the detail required in a decision prohibiting by effect agreement is on a different level.[8]

Moving on to the procedural aspects of competition law, it must be underlined that cartels are truly difficult to spot and enforce. The undertakings involved in a cartel agreement are usually aware that they are committing an illegal pursuit, which explains their intention to hide all the possible evidence. There are several ways on how to detect a cartel. To mention but two, first, competition authorities have at their disposal strong investigatory powers. Pursuant to Regulation 1/2003[9], the European Commission is entitled to conduct sector investigations, to request information, to take statements and to conduct inspections in business and non-business premises.[10] The last mentioned investigatory power, right to perform inspection, is a very effective, yet highly controversial investigatory tool.[11]

Second, competition authorities may be given a helping hand by a whistle-blower. Under the leniency program, one party of a cartel agreement "*blows a whistle*", in other words, it approaches a competition authority by giving them evidence on the existence of cartel. The whistle-blower is then pardon from a part or whole of the fine for the cartel.[12]

2.1. Bid rigging as a form of horizontal agreements

One of the competition-related concerns in the field of public procurement is bid rigging.[13] Zooming in on cartels in procurement procedures, bid rigging is considered to be a hard-core cartel. Even more, it may be understood as one of the most serious form of competition law

[8] Mária Patakyová, 'Cieľové vertikálne dohody' (Conference Aktuálne otázky súťažného práva v Európskej únii a na Slovensku, Bratislave, 2015)' 59.

[9] Council Regulation (EC) No 1/2003 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2003] OJ L1/1 ("Regulation 1/2003").

[10] Articles 17-21 of Regulation 1/2003.

[11] See, for instance: Adam Steene 'Nexans, Deutsche Bahn, and the ECJ's Refusal to Follow ECHR Case Law on Dawn Raids' (2016) 7 JECLAP 180.

[12] Richard Whish and David Bailey (n 6) 281.

[13] Albert Sanchez Graells, 'Public Procurement and Competition: Some Challenges Arising from Recent Developments in EU Public Procurement Law' (2013) < http://ssrn.com/abstract=2206502> accessed 14 August 2019, 4.

infringements, as it destroys both the competition on the market and the incentives under public procurement law.

As presented by the Dutch competition authority, bid rigging often results in higher prices or lower quality. Hence, contracting authorities pay too much for too little.[14]

From a practical point of view, bid rigging is usually hidden from the sight of the authorities. The undertakings agree among themselves who would be the winning participant in the particular procurement. In order to cover their behaviour, there are usually more participants in the tendering procedure, not only the intended winner. Rather the opposite, it appears at first glance that undertakings compete against each other, whereas in reality the winner is set in advance and the other participants put so called cover bids into the process.[15]

The principle of rotation may be based on various factors. For example, the geographic division of market may be implemented in this manner.

Apart from pure bid rotation, bid rigging can also take another forms. For example, the parties could agree on compensation payments. Plus, bid rigging may be achieved not only through agreements, but also through information exchange, which may reveal the intention of a firm to bid as well as the price and conditions of the bid.[16]

In any case, the breaking point of a cartel lies in the participants. It is assumed that there is a need for a majority of tenderers to collude, otherwise the bid rigging will be inefficient.[17]

2.2. Bid rigging and its enforcement

Cartels related to tendering procedures may have several forms. All of them are usually well hidden and difficult to spot. Giannino presents a way

[14] Netherlands Competition Authority, 'Bid rigging, Detecting and preventing collusion in procurement' (acm.nl, 2010) < https://www.acm.nl/sites/default/files/old_publication/publicaties/6726_brochure%20bid-rigging%20.pdf> accessed 25 August 2019.

[15] Kalesná (n 7) 23, 27.

[16] Ritter (n 20) 2.

[17] D. Raus, A. Oršulová, *Kartelové dohody* (1st edn, C.H.Beck 2009) 122, in Katarína Kalesná, 'Tendrové kartely a ich špecifiká' in Kristína Považanová (ed), *Aktuálne otázky súťažného práva v Európskej únii a na Slovensku* (Univerzita Komenského v Bratislave, Právnická fakulta, 2015) 23, 27.

on how to detect and investigate a bid rigging.[18] A competition authority may detect certain abnormalities on the market, which may lead to a suspicion that a cartel has taken place. Subsequently, external evidence is searched in order to support the suspicion. The existence of the cartel may also be supported by internal evidence, for example by decision-making procedure within the undertaking at stake. If the undertaking participated in certain public procurements, but not in the other, why was the undertaking absent in the latter and not in the former? Last but not least, there is always a room for undertaking's defence, in which the undertaking may present reasons for its activity (or lack of it).[19]

The Dutch competition authority presents several signs which serve as a smoking gun, for example: bids of certain firms in certain regions, which were never the winning bids; few bidding firms; subcontracting to competitors; striking pattern of winners; certain bids being very brief; winner not accepting the contract and rather working as subcontractor. Apart from these signs regarding bid patterns, there are also signs regarding pricing or behaviour of firms.[20]

3. Algorithms and Artificial Intelligence

Utilisation of software has significantly changed the *modus operandi* of states, public bodies, firms and people in general. The change has been shifted to a new level by employment of artificial intelligence. How has the use of AI and algorithms influenced the bid rigging?

3.1. AI and algorithms as a tool for detection

As mentioned above, abnormalities on the market may be one indicator of a cartel. Naturally, these abnormalities may be better detected with algorithms and AI. In the following text, we will briefly present several methods of bid rigging's detection.

One of the basic methods of detection lies in the use of econometrics and statistics. A specific tool for detection of cartels was presented by Porter and Zona. The tool was related to the knowledge of relationship

[18] Michele Giannino, 'Collusion in Public Contracts Procurement: Suppliers of School Cleaning Services Fined for Bid Rigging (Italy)' (2017) 8 Journal of European Competition Law & Practice 247.

[19] ibid 248-250.

[20] Netherlands Competition Authority (n 14).

between bids and costs. The bids presented by undertakings involved in bid rigging were not so strictly related to the measurement of the costs.[21]

Not all the tools are based on econometrical and statistical methods. Indexing methods may be used as well. These methods concentrate on spotting "*suspected*" markets based on certain signals or signals sets. For example, Harrington[22] showed a set of indicators based on price behaviour and market shares of undertakings. Subsequently, the indicators may be used for application of screening tests which may reveal a cartel environment, or, alternatively, an environment after a cartel was broken.[23]

Zooming in on the real-functioning methods, one can take the example of the Netherlands Competition Authority. The so called Competition index takes into account nine indicators, which can be split into four main categories: degree of organization; prices; concentration; dynamics. In order to get a result, indexation methodology is used. Numbers of the nine indicators *per* industry are standardized. Weighted average of such numbers results in a ranking list of industries.[24]

A new level of bid rigging detection may be brought by wide implementation of E-procurement.[25] A significant advantage of moving the tendering procedure online is the availability of data for further analysis. The Artificial intelligence may be well employed in the processing of the data. Various important information may be learned through such data processing, for example personal ties, market concentration, geographical variability of ordered contracts etc.[26]

[21] R.H. Porter, J.D. Zona, 'Ohio School Milk Markets: An Analysis of Bidding' (2017) 30 RAND J. Econ., 263 in Andrzej Foremny and Wojciech Dorabialsky, 'Review of collusion and bid rigging detection methods in the construction industry' (Creative Construction Conference, Ljubljana, 2018) 946, 947.

[22] Joseph E. Harrington, Jr. 'Behavioral Screening and the Detection of Cartels' (EU Competition Law and Policy Workshop/Proceedings, 2006) < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.4196&rep=rep1&type=pdf> accessed 30 July 2019.

[23] Foremny and Dorabialsky (n 21) 946, 948.

[24] Lilian Petit, 'The Economic Detection Instrument of the Netherlands Competition Authority' (2012) NMa Working Papers, No 6 < http://ssrn.com/abstract=1992774> accessed 25 August 2019, 17.

[25] Sanchez Graells (n 13) 36.

[26] Foremny and Dorabialsky (n 21) 946, 952.

3.2. AI and algorithms as a tool for collusion

In general, digitalised markets have many advantages from competition point of view. Markets are more transparent and more effective.[27] Digitalised markets brought new products to customers, for example social networks, as well as they make already existing products more available. The latter is related, for instance, to online shopping.

On the other hand, digitalised markets are accompanied by various competition threats. For instance, algorithms may change structural characteristics of the industry, i.e. number of firms on the market, creation of barriers to entry, market transparency and frequency of interactions. The actual effect of algorithms depends on the industry, however, regarding the number firms, new technologies can make the number of competitors less relevant factor for collusion.[28]

Moreover, availability of prices online may facilitate the sustainability of a cartel. If the market is transparent, cartelists do not need sophisticated tools for control of other cartelists' compliance with the cartel. Necessary information is easily and publicly available. Plus, the combination of availability of market data and machine learning may leave to predicting the rivals' actions and forecasting a deviation from a cartel before it actually takes place.[29]

Besides, digitalised markets may lead to new competition law infringements. For instance, harvesting of data on large scale by a dominant undertaking can result in abuse of dominant position in this specific form. We may mention Facebook, which was under scrutiny by the German competition authority and the decision was issued at the beginning of 2019.[30]

[27] Ariel Ezrachi and Maurice E. Stucke, 'Artificial Intelligence & Collusion: When Computers Inhibit Competition' (2015) Oxford Legal Studies Research Paper No. 18/2015, 1 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2591874> accessed 31 July 2019, 3.

[28] OECD, 'Algorithms and Collusion - Background Note by the Secretariat' (EOCD, 2017) <https://one.oecd.org/document/DAF/COMP(2017)4/en/pdf> accessed 25 August 2019, 19.

[29] ibid 20.

[30] Bundeskartellamt, 'Bundeskartellamt prohibits Facebook from combining user data from different sources' (Bundeskartellamt.de, 7 February 2019) < https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html> accessed 31 July 2019

Once undertakings dispose with large scale data, they may implement data analysis tools and self-learning mechanisms in order to enhance their business strategy.[31] The use of specific algorithms has already resulted in anticompetitive practices, for instance in the case of price fixing by Amazon Marketplace in USA. This case is dated to 2015.[32]

3.2.1. Four categories of collusion with the help of computers

Returning to the issue of collusion, Ezrachi and Stucke[33] elaborated, among others, on the following questions: how may computers be involved in the process of collusion? Is competition law strong (and flexible) enough to cover these types of Article 101 infringements? In answering these questions, they presented four categories of collusion.

The first category is characterised by using computers as "*Messengers*". In this case, computers are used to execute the will of humans who decided to collude. For example, a software is created which serves as a forum to exchange sensitive information. The use of competition law is quite straightforward and the evidence on the parties' intent is not necessary.[34]

The second category is characterised as "*Hub and Spoke*". This form is based on a use of a single algorithm which determines the price. If several undertakings use the same algorithm, it will logically lead to the similar prices charged by these undertakings. The result is, therefore, the same as the implementation of a price cartel. An evidence on the intention of the undertakings using the same algorithm may be used.[35]

The third category is named as "*Predictable Agent*". In this scenario, undertakings use not the same, but similar algorithms. No agreement among the parties is proved and it even does not have to exist. If similar algorithms are implemented throughout an industry, anticompetitive effects may follow. However, in this case, such "*collusion*" is not, as presented by Ezrachi and Stucke, automatically illegal. A proof of intention

[31] Ezrachi and Stucke (n 27).

[32] Department of Justice, 'Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution' (Justice.gov, 6 April 2015) <http://www.justice.gov/atr/public/press_releases/2015/313011.docx> accessed 31 July 2019

[33] Ezrachi and Stucke (n 27).

[34] ibid 10-14.

[35] ibid 14-16.

is required according to the authors. Moreover, use of similar algorithms may lie directly on the edge between tacit collusion and conscious parallelism.[36]

Within the EU environment, this type of behaviour may be relevant within the concerted practice analysis. Yet, again, one would need to distinguish between collusive and non-collusive behaviour. The concerted practice would take place if a practical cooperation between parties is knowingly substituted for the risks of competition. Therefore, the aims which are intended to be reached, together with the economic and legal context, shall be assessed.[37]

The final, fourth category, is connected to "*Autonomous Machines*". Software, backed up by artificial intelligence, determine the price independently from the will of the undertakings, with the aim of optimisation of profit. If there are more such machines on the market, they may communicate between each other and, through self-learning and experiment, commence to collude, totally independently from the will of the undertakings. In such case, liability is, in the view of the authors, unclear.[38]

3.2.2. Bid rigging with the help of computers

It is highly probable that collusive practices in tendering procedures may be fuelled by algorithms. As stated by OECD, collusion may be facilitated by monitoring algorithms, parallel algorithms, signalling algorithms or even self-learning algorithms.[39] All of these may be virtually applied in bid rigging.

Addressing the four categories, it is undoubted that tenderers use certain types of algorithms when calculating the costs of providing of the particular goods or services, and, consequently, their bids. It cannot be excluded that participants will use a same software to calculate their costs; such behaviour might fall into the second category.

[36] ibid 16-22.

[37] Judgment of 4 June 2009, *T-Mobile Netherlands and Others*, C-8/08, EU:C:2009:343, paras 26, 27.

[38] Ezrachi and Stucke (n 27) 22-25.

[39] OECD, 'Algorithms and Collusion - Background Note by the Secretariat' (EOCD, 2017) <https://one.oecd.org/document/DAF/COMP(2017)4/en/pdf> accessed 25 August 2019, 24-32.

What seems problematic from enforcement perspective is the case when several undertakings develop their own software, however, the result will be so similar as to lead *de facto* unification of bids. This may be done, for instance, by outsourcing the creation of algorithms to the came IT programmers.[40] Such situation could fall into the third category.

Without an actual agreement between the parties, it might be fairly difficult to establish concerted practices between them. To prove the intention of the parties may be very difficult in practice. Naturally, one must distinguish between normal behaviour of undertakings on the one hand, and forbidden collusive behaviour on the other. Moving towards transparent procurement procedures, which are in general very beneficial, one can imagine the situation in which algorithms, well-fed with data, may determine the bids of competitors, even without the algorithms being exactly the same.

4. Conclusion

Constant penetration of technologies can hardly be slowed down. One shall learn how to master them, otherwise there is a risk of serious negative externalities. Increase use of algorithms and artificial intelligence by competition authorities mean that they may conduct sector studies to define the problematic industrial sectors as well as that they may spot collusion easier than before.

On the other hand, AI is more and more used by undertakings. It would be naïve not to expect them to utilise algorithms also for illegal purposes, collusion included. Algorithms may facilitate performance and sustainability of “traditional” types of collusion. However, they may lead to creation of new forms. It seems that development of similar pricing algorithms by various undertakings should be focused on in particular. Enforcement of such practice will not be easy, hence, competition authorities might stand before a challenge how to prove that, in the absence of a provable agreement, a collusive behaviour has taken place.

References

[40] ibid 27.

- Bundeskartellamt, 'Bundeskartellamt prohibits Facebook from combining user data from different sources' (Bundeskartellamt.de, 7 February 2019) < https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html> accessed 31 July 2019
- Chalmers, Damian; Davies, Gareth and Monti, Giorgio, *European Union Law* (3rd edn, Cambridge University Press 2014)
- Department of Justice, 'Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution' (Justice.gov, 6 April 2015) < http://www.justice.gov/atr/public/press_releases/2015/313011.docx> accessed 31 July 2019
- Demčák, Peter, 'Dohody obmedzujúce súťaž' (Conference Efektívnosť právnej úpravy ochrany hospodárskej súťaže – návrhy de lege ferenda, Bratislave, 2017)
- Ezrachi, Ariel and Stucke, Maurice E., 'Artificial Intelligence & Collusion: When Computers Inhibit Competition' (2015) Oxford Legal Studies Research Paper No. 18/2015, 1 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2591874 > accessed 31 July 2019
- Foremny, Andrzej and Dorabialsky, Wojciech, 'Review of collusion and bid rigging detection methods in the construction industry' (Creative Construction Conference, Ljubljana, 2018)
- Giannino, Michele, 'Collusion in Public Contracts Procurement: Suppliers of School Cleaning Services Fined for Bid Rigging (Italy)' (2017) 8 Journal of European Competition Law & Practice 247
- Harrington, Joseph E. Jr., 'Behavioral Screening and the Detection of Cartels' (EU Competition Law and Policy Workshop/Proceedings, 2006) < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.4196&rep=rep1&type=pdf> accessed 30 July 2019
- Kalesná, Katarína, 'Tendrové kartely a ich špecifiká' (Conference Aktuálne otázky súťažného práva v Európskej únii a na Slovensku, Bratislave, 2015) 23
- OECD, 'Algorithms and Collusion - Background Note by the Secretariat' (EOCD, 2017) <

https://one.oecd.org/document/DAF/COMP(2017)4/en/pdf> accessed 25 August 2019

- Patakyová, Mária, 'Cieľové vertikálne dohody' (Conference Aktuálne otázky sú-ťažného práva v Európskej únii a na Slovensku, Bratislave, 2015) 59
- Patakyová, Mária, 'Vplyv Európskej únie na legislatívu Slovenskej republiky v oblasti hospodárskej súťaže' (Conference Míľniky práva v stredoeurópskom priestore, Častá-Papiernička, 2015) 124
- Petit, Lilian, 'The Economic Detection Instrument of the Netherlands Competition Authority' NMa Working Papers No 6, 2012 < http://ssrn.com/abstract=1992774> accessed 25 August 2019
- Ritter, Cyril, 'Joint tendering under EU Competition Law' (2017) <http://ssrn.com/abstract=2909572> accessed 14 August 2019
- Sanchez Graells, Albert, 'Public Procurement and Competition: Some Challenges Arising from Recent Developments in EU Public Procurement Law' (2013) < http://ssrn.com/abstract=2206502> accessed 14 August 2019
- Steene, Adam, 'Nexans, Deutsche Bahn, and the ECJ's Refusal to Follow ECHR Case Law on Dawn Raids' (2016) 7 Journal of European Competition Law & Practice 180
- Whish, Richard and Bailey, David, *Competition Law* (7th edn, Oxford University Press 2012) 124

Short biography of the author

Mária T. Patakyová is assistant professor at Institute of European Law, Faculty of Law, Comenius University in Bratislava, Slovakia. She completed master studies and PhD studies at Faculty of Law, Comenius University in Bratislava. She is a graduate of the Cambridge Diploma in British Law and European Union Law. She lectures several courses, mostly related to EU law, she also participates in moot courts (CEEMC, ELMC) as a (main) coach.

Part of her studies were done at Faculty of Law, Ljubljana University, Slovenia. She was also studying and doing research at Tilburg Law School, the Netherlands.

Regarding the research, she has focused mainly on protection of human rights in Europe, business human rights, national and European competition law (including zero-price markets), internal market law, migration law and consumer law. She has published in Journals and Proceedings from conferences both in Slovakia and abroad.

Fear the robots? – Attitudes from the supply chain

István Pesti-Farkas* – Zoltán Szegedi

Abstract: As part of the results of a questionnaire from January 2019, on the sample of 111 answers, a research had been performed in order to highlight the human aspect of the technological change. Different servicers are waiting the new (even disruptive) technologies on a different way, therefore it is worth to have a common understanding on the beliefs, especially on the fear…

Keywords: Industry 4.0, brewers, supply chain, human workforce, robotics

1. Introduction

As in the last centuries, the development of the industry had several revolutions. After the invention of the steam power utilization, the mass production and the automatization (as you can see on the first figure), the Industry 4.0 is about the connectivity of the devices and environment, the application of the sensors. The improved processes sometimes replacing, sometimes assisting the daily tasks of the human workforce. The aim of the research is to call the attention to the attitudes regarding to the robots and automatization, as part of the above.

The scaling of the research had been set as follows: the responders had been asked to pick one (or more) challenges from the offered list, therefore it shall be regarded as nominal scale.

The statistical reliability of the used data had been validated by the Pearson Correlation and as the values had reach the level of confidence, (the correlation had been proved as significant) they had been selected as basic for the complete analysis.

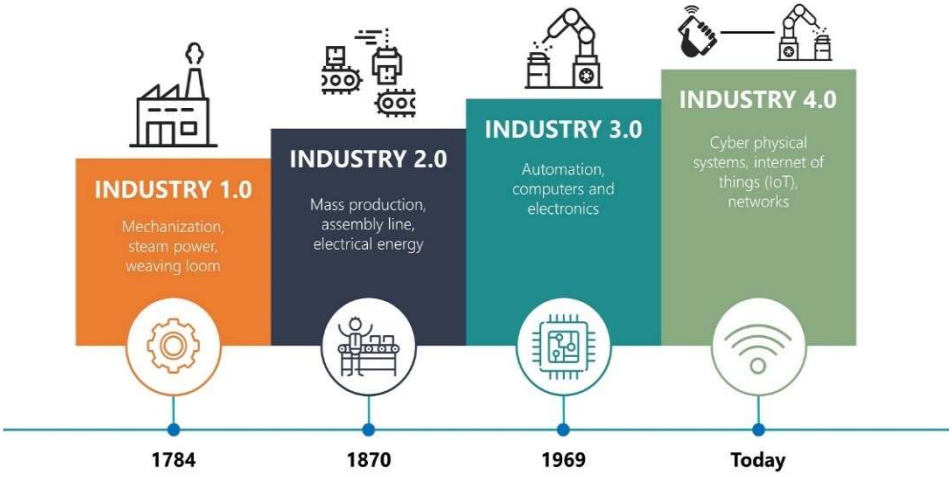
Importance of the topic cannot be questioned: the latest industrial revolution has a clear effect on the manufacturing environment and processes, because of the connected items can share their big data and let it analyzed real time, which lead to proper, faster and efficient decisions. The revolution has effect on the human workforce as well,

* Correspondent author, scientific.pesti@gmail.com.

because the current blue (or even white) collar workers` jobs seems excellent training area to the learning robots and for the artificial intelligence, which may result changes in the employment on long term.

And last, but not the least, the current status caused new solutions require investments as well, but they offer as compensation the possibility of higher-than-ever return.

Figure 1: Industrial revolutions



Source: http://trilliummfg.ca/the-rise-of-big-data-and-industry-4-0/

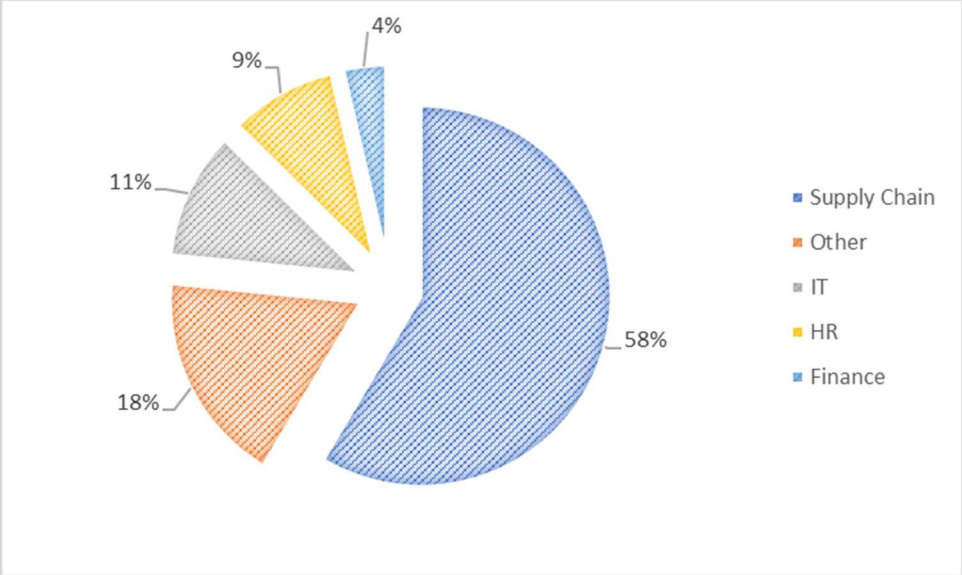
2. The process of the empirical research

The questionnaire of the research had been finalized in December 2018 and as soon as it had been approved, it was sent out from the e-mail address as scientific.pesti@gmail.com. 350 professionals had been reached out directly and the Corvinus Alumni Club on LinkedIn (with 3739 members) beside of the Hungarian Business Society (with 6478 members) and Procurement People Network (with 6725 members). Approximately there was 17.000 professionals asked to fill out the survey, so compared with the number of arrived answers (111 pc), the answer rate is 0,65%. One representative of an FMCG manufacturer had noted that their internal policies do not allow them to reply and one brewery supplier noted his concerns regarding to the GDPR. All of the responders had been coded with the value of „Company1-Company111”.

2.1. Responders

As it is visible on the first figure below, the distribution of the responders shows a clear picture on the weight of the answers. As it is visualized on the second figure below, 58% of the responders are working on the field of supply chain, 18% of them noted „other" area, because the engineering/operation activities had not been listed. The HR and IT field are represented approximately in the same portion, by 10-10%. The finance professionals are part of the answers in 4%.

Figure 2: Distribution of professional area of responders



Source: Own creation

3. Analysis

3.1. Method

From the multivariate statistical analyses - which are standard for high volume of data, we have selected the factor analysis. Our aim was to understand the variables and group them. There are correlations between the variables, they can be stated based on the directly unidentified background variables, as factors. The described variants' linear combination creates new variants. As first step, we made the covariance matrix of the standardized variants, where the connection of the given variant had been set with the others. Than the factor extraction had been made, the identification of the factors. We had made the standard variants matrix, where the connection of each variant to another one had been identified. Later, the factor extraction had happened, so we had identified the factors. The weight estimation of the factors had been made based on the SPSS analysis: the more-than-1 values had been considered from the decreased ordered values. As the own value of the factor shows the percentage of the variable from the total variance, therefore the less the own value of the factor, the less it contributes to toe total explained variance. 1.00 had been chosen as limit, because under this value, the factor does not explain its own variance. The understanding and naming had been performed in accordance with it, so there had been the following factors created: data analysis, robotics, logistics, office usage and customer management. The analysis had been performed because of exploratory nature, the overall goal of it was to create the group of the variables, which can be the basic for the further structure of the other answers as well. The factors had been rotated in order to gain additional data contain. The analysis had been validated with Kaiser criteria and the KMO value had been controlled. The KMO values show that the variants can be regarded as proper, so can be selected for factor analysis. The table can be divided into three main units: the first one shows the Initial Eigenvalues, the second one the Extraction Sums of Squared Loadings, the third one the Rotation Sums of Squared Loadings. The total row shows the own value, the „% of Variance" the percentage of explained variance within the total variance, the „Cumulative %" row shows the total variance. As it can be applied in case of lower measurement level variables, we had considered the application of crosstabulation, which is a table for the description of the correlation between the variants. In the created matrix, there are two (or more) nominal or ordinal variant value common distribution had been visualized, so shows the combinations of the values of the variants. Obviously, the table had been created with those cells,

which contains all combination of all values of the two variants. These cells are showing the correlation, but the above referred percentage and numeric values are not efficient to describe the correlation between the variants, therefore the chi-square test had been applied as well. The Null-hypothesis was that there is no correlation between the variants. As the chi-square value related significance level is lower than 0,05, the Null-hypothesis had been rejected.

3.2. Factors

In order to understand the big picture from the answers to the questionnaire, the answers on the Industry 4.0 solutions had been processed at first. We had included into the listed items those ICT and social media solutions, which are able to show the attitude of the responders to the topic. The factor analysis resulted 5 factors, where the information exists in a compressed, but not lost format. The first factor is the group of those companies, which already are applying this kind of solutions for data analysis, the processing and analysis are part of the daily tasks. The second factor is the group of those companies, which - based on their answers on the solutions - are familiar with the basics of robotics (eg. From 3D printing, etc.), with its substantial principles and daily operation of the robots, not necessarily in their own operation. The third factor is the group of those companies, which are focused on logistics. This significantly separated group had been categorized because of the similar task and position of these companies. The RFID and scanner usage are already existing on the market, but the given answers had highlighted the previous processes and tools of the old manufacturing technologies and their development, which shall be already considered as out-of-date. The fourth factor is the group of those digital business companies (having office applications), which are indirect processes, not related directly to the manufacturing of production, like HR or facility management. It became visible that the e-invoicing and the online collaboration tools are known and used in front of the responders, but only at one part of the responders' group. It was interesting to see that the cloud-based solutions are in this category as related question, but their usage is much more than a standard data storage function. The last, fifth factor is the customer management focused companies, as the mobile- and social applications are known in a group of firms. The automatized customer service and the digitalized customer management

might part of the daily operation of those companies, which are still using the tools and solutions of the previous industrial revolutions for material movement or inventory management. Overall, the reason of the selection of the factors was to reflect to their competency regarding to the ICT solutions, because the Industry 4.0 is about the application of them, The link between the factors is the maturity: it varies from the basic, office used technologies until the up-to-date, state-of-the-art solutions. The hypothesis was that those companies, which are operating on the field of logistics, have more positive attitude to the robots as Industry 4.0 solution than other companies from the business, including the fact that the robots will assist human workforce in the operation, not replace.

3.3. Results

In relationship with the new digital technologies, in the questionnaire, the responders had been asked to note, which are the biggest challenges for them, with the following options: Available professional expertise, there shall be new workplaces, Robots shall replace the human workforce, Robots shall support the human workforce There was a relevant statistical correlation in the data analysis category, at the available professional expertise and the belief in new workspace creation. It can be interpreted as those, who are skilled in data analysis are considering the professional expertise as key element to the further, robot assisted operation and the new opportunities will create new workspace because of the increased and more efficient processes. In logistics category, there is a correlation with new workplaces and support of the human workforce, what is logically acceptable as the whole supply chain is currently influenced (beside of the manufacturing) the most by these new, disruptive technologies. In digital business category, the correlation exists with the available professional expertise as challenge, what refers to the fact, that the digital business solutions (eg. Office softwares, etc.) are representing the first steps in the digital era, do not request deeper ICT knowledge.

4. Conclusion

Independently from its role within the whole supply chain (whether is it a direct/indirect supplier/servicer of a brewery), the responders had been categorized based on their robotics attitudes. Based on this, their challenges had been analyzed towards the Industry 4.0 solutions: there

are some activities (eg. Digital business solution application or data analysis), which do not require specific, deep ICT knowledge, therefore their attitude to the robotics can be regarded as neutral, they are mostly interested in the professional expertise as the way of managing a robot supported business. But the hypothesis of the research had been validated and confirmed: the logistic activity related answers had showed that they are more tolerant to the sensors caused changes, they believe – based on their current knowledge and experience – that the robots are going to support their daily work, they can not replace them. Even they can see the increased number of developments as autonomous vehicles, automatic processes and automated warehouses, they consider themselves as substantial part of the movement of goods. They have no fear from robots at all.

References

All above data, chart, figure and analysis are part of the Authors` own research.

Short biography of the authors

Prof. Dr. habil. Zoltan Szegedi is the Professor of Logistics & SCM at Szechenyi Istvan University, Dept. of Marketing & Management, and Head of Section Organisation & Management.

Istvan Pesti-Farkas holds an MSc degree in logistics management. He is a doctorate candidate at the Regional- and Business Economics Doctorate School at the Szechenyi Istvan University in Gyor.

AI Risk Assessment Tools: The Trojan Horse of the Criminal Justice System

Laura Stănilă*

Abstract: Risk-assessment tools are Artificial intelligence (AI) systems, which are increasingly used to ease the decision-making process for humans in criminal justice system, especially in different phases of a criminal trial: pre-arrest phase, conviction phase, parole, etc. The number of countries using this type of tools in order to ensure objectivity of the police, prosecutors or judges decision process and, in the same time to ease this process is growing. Although risk assessments tools were declared to have a positive impact on the rights of individuals accused and convicted of crimes, recent researches have shown flaws and errors in their decisions, raising concerns on the fact that they might be producing harmful effects on the rights of indicted or convicted persons. The causes of such damaging outputs of the AI systems are worth to be analysed due to their long-term impact on the criminal justice system. If the algorithms, which are fed with data provided by humans, are not "cleaned" of the discriminatory patterns, the use of such AI tools will produce more harm than benefit for the justice system. Another debate may be on the mandatory use of AI risk assessment tools by the judiciaries, because of recent research offering alarming results on their errored function or output data.

Keywords: risk-assessment tools, criminal justice system, criminal risk, discrimination

1. What Risk Assessment AI Tools really are?

Recently our society has witnessed an explosion in the use of algorithms in the public sphere especially in the United States, the US criminal justice system moving as well, from predictive policing to risk assessment in the corrections system[1].

* Senior lecturer, West University Timișoara, Faculty of Law, laura.stanila@e-uvt.ro.

[1] D. Kehl, P. Guo and S. Kessler, 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative' (*Berkman Klein Center for Internet & Society, Harvard Law School*, 2017) <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041> accessed 10 May 2019, 3.

The verification of the risk factors most predictive of adult offender recidivism and identification of the actuarial instruments best suited to that end have major implications for corrections policymakers, practitioners, and program evaluators[2]. Nowadays, when the management of prisons must met the standards of cost-effectiveness while dealing with the increase in incarceration rates, it has been pointed out that maximum security prisons be reserved for the highest risk offenders while the design of effective offender treatment programs is highly dependent on knowledge of the predictors of recidivism.[3] But still, the issue of misbehaving algorithms remains, the debate becoming even more fierce, as fundamental rights of the person could be in peril.

Criminal doctrine identifies 19 (nineteen) risk assessment instruments in US criminal system (all of them being evaluated in 53 studies published between 1970 and 2012). The risk assessment instruments varied widely in the number, type, and content of their items, but generally were characterized by static risk factors to the exclusion of dynamic risk factors and protective factors. But non of these risk assessment instruments emerged as producing the most accurate risk assessment in U.S.[4]

There are a lot of types of recidivism risk assessment instruments and they may be distinguished in terms of their approach, item type, and item content. Desmarais, Johnson and Singh identified two broad categories related to approaches used by risk assessment instruments: actuarial and structured professional judgment.

a) The actuarial approach represents a mechanical model of risk assessment in which offenders are scored on a series of items that were most strongly associated with recidivism in the development samples. Then, total scores are cross-referenced with actuarial risk tables.

b) The structured professional judgment approach guides assessors to consider a set number of factors that are empirically and theoretically associated with the outcome of interest. Though individual items are scored, assessors ultimately make a categorical judgment of risk level

[2] P. Gendreau, T. Little and C. Goggin, 'A meta-analysis of the predictors of adult offender recidivism: What works!' (1996) 34 Criminology <doi: 10.1111/j.1745-9125.1996.tb01220.x> accessed 10 March 2019, 575.

[3] ibid 575.

[4] S. L. Desmarais, K. L. Johnson and J. P. Singh, 'Performance of Recidivism Risk Assessment Instruments in U.S. Correctional Settings' (2016) 13 (3) Psychological Services 216.

(e.g., low, moderate, high) based on their professional judgment rather than using total scores.[5]

Risk assessment tools, measures and techniques are also classified within a developmental framework: first generation, second generation and third generation:

a) first-generation techniques are based on clinical intuition and professional judgment.

b) second-generation assessments are actuarial in nature. They are based on standardized, objective risk prediction instruments, such as the Salient Factor Score (SFS), that are based almost entirely on static criminal history items. These kinds of measures provide little direction for classification and treatment decisions because the fixed nature of the items does not allow for changes in the offender's behavior to be reflected on subsequent retesting.

c) third generation instruments are of two types:

c.1 – prediction is based on dynamic factors (e.g., Community Riskmeeds Management scale; Level of Service Inventory (LSI-R); the Wisconsin system), which assess a wide range of criminogenic needs.

c.2. - prediction is based on personality test scales in the antisocial personality/ sociopathy/psychopathy content area which are dynamic in nature but do contain static items. (e.g., the MMPI Pd scale, the Psychopathy Checklist - PCL-R); the Socialization scale – SOC - of the California Personality Inventory - CPI)[6].

In United States authorities prefer 6 (six) risk assessment AI tools using them to assess key risk factors in adult and youth correctional populations and to provide decision support for practitioners, risk for recidivism, in order to support various decision points in the criminal justice system (pretrial, community supervision, prison intake, etc.).

In the following the most used AI risk assessment tools are going to be shortly presented:

a) Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)

This AI tool was developed by Northpointe Institute for Public Management, Inc. in 1998. This statistically-based tool was designed to assess key risk and needs factors in adult and youth correctional populations and to provide decision support for practitioners charged with

[5] ibid 207.

[6] Gendreau, Little and Goggin (n 2) 577-578.

case planning and management. COMPAS can assess four types of risk - general recidivism, violent recidivism, non-compliance, and failure to appear - for use at a variety of decision points in the criminal justice system.[7]

b) Inventory of Offender Risk, Needs, and Strengths (IORNS)

IORNS was created by Dr. Holly Miller in 2006 as an offender assessment of static risk, dynamic risk/need, and protective strength factors. The tool is complimented by several subscales for specific assessments in the areas of violent and sexual criminal behavior.[8] IORNS has been described as demonstrating potential as a self-report measure of static risk, dynamic risk and treatment/management needs, and protective strengths. IORNS examination with several additional samples of offenders is warranted to further validate the measure. Additionally, studies that further examine the predictive power of the IORNS, especially to predict re-offense, are warranted in order to substantiate its use in the prediction of general, violent, and/or sexual recidivism[9].

c) LSI-R (Level of Service Inventory-Revised) and LS/CMI (Level of Service/Case Management Inventory) LS/RNR (Level of Service/Risk, Need, Responsivity)

LSI-R was first developed in 1995 by Don Andrews and James Bonta as a third generation approach to offender risk assessment. As shown before, third generation tools assess static and dynamic risk and needs factors in the evaluation of an offender's risk for recidivism and assess whether the offender may be amenable to community intervention/treatment for the purpose of risk reduction. The LS/CMI is the fourth generation revision of the LSI-R that assesses offender risk, needs, and responsivity (RNR) to inform case planning via a built-in case management system. The LS/RNR is similarly comprised of the updated

[7] T. Brennan, W. Dieterich and B. Ehret, 'Evaluating the Predictive Validity of the Compas Risk and Needs Assessment System' (2009) 36 Criminal Justice and Behavior <DOI: 10.1177/0093854808326545> accessed 18 March 2019, 22-23, also see C. Matacic, 'In the United States, computers help decide who goes to jail. But their judgment may be no better than ours' (*Science,* 17 January 2018), <https://www.sciencemag.org> accessed 18 March 2019.

[8] H. A. Miller, 'A Dynamic Assessment of Offender Risk, Needs, and Strengths in a Sample of Pre-release General Offenders' (2006) 24 Behavioral Sciences and the Law <https://onlinelibrary.wiley.com/doi/abs/10.1002/bsl.728> accessed 20 March 2018, 772.

[9] ibid, 780.

risk, need, and responsivity scales, but offer these separately from the LS/CMI case management system for organizations already equipped with established case management systems of their own. A quite important number of studies confirm predictive validity of LS/CMI with recidivism and prison adjustment, no matter the type of the offender (i.e., adults, juveniles, natives, females).[10]

LSI-R is in use also in other countries such as Scotland, and in about 20 probation services in England, Wales and the Channel Islands. It is the product of about 20 years' development, and a considerable amount of research has been carried out on its psychometric properties and its capacity to predict reconviction and various other correctionally-relevant outcomes in North America.[11]

d) ORAS (Ohio Risk Assessment System)

ORAS was developed in 2006 by the University of Cincinnati Center for Criminal Justice Research at the request of Ohio Department of Rehabilitation & Correction. It is a system meant evaluate offender risk, needs, and responsivity to be use statewide. ORAS was meant to be used at various decision points in the criminal justice system (i.e., pretrial, community supervision, prison intake, reentry) to facilitate communication and continuity across criminal justice agencies. Although the data collection period gathered information on over 1,800 offenders in Ohio, studies have shown it would be imprudent to assume that the findings are representative of all offenders in Ohio and, although the samples were gathered from specific populations, certain types of cases may be underrepresented in the population (e.g. sex offenders, Hispanic offenders, female offenders). The underrepresentation in the population has led to small numbers of these types of offenders in the sample[12].

e) OST (Offender Screening Tool)

OST was developed and implemented in 1998 by the Maricopa County Adult Probation Department and David Simourd, being validated for

[10] Gendreau, Little and Goggin (n 2) 590.

[11] P. Raynor, J. Kynch, C. Roberts and S. Merrington, 'Risk and need assessment in probation services: an evaluation' (2000) 211 Home Office Research Study <https://www.researchgate.net/publication/267419138_Risk_and_Need_Assessment_in_Probation_Services_An_Evaluation/download> accessed 12 December 2018, viii.

[12] E. Latessa, P. Smith, R. Lemke, M. Makarios and C. Lowenkamp, 'Creation and validation of the Ohio Risk Assessment System: Final report' (2009) <https://www.assessments.com/> accessed 20 March 2019, 39.

statewide (US) use in 2003 and fully implemented statewide in 2005 pursuant to Arizona Supreme Court Administrative Order 2005-12[13]. It was also revalidated in Arizona in 2008. In 2009, the Arizona Judicial Council adopted the use of a statewide standard presentence report that incorporates the criminogenic risks identified in the OST[14]. Still, studies have shown that obtaining quality information is the key factor for an accurate result of using this tool. "Quality assessment information is essential if the assessment tool is going to be used to inform decisions".[15]

f) STRONG (Static Risk and Offender Needs Guide)

In 2008, the Washington State Department of Corrections implemented there an automated offender assessment and case planning system with the research services of Washington State Institute for Public Policy and technical assistance from Assessments.com, following the adoption of Washington State's Offender Accountability Act in 1999 which identified the need to "reduce the risk of reoffending by offenders in the community." STRONG is an automated system including the Static Risk Assessment and an Offender Needs Assessment, which is used to identify offender needs and protective factors for use in case planning. It is a fourth-generation risk and needs assessment system and presents certain advantages:

- Increased predictive accuracy;
- Prediction of three types of high-risk offenders—drug, property, and violent;
- Increased objectivity;
- Decreased time to complete the assessment;
- Accurate recording of criminal history for use with other Department of Corrections reporting requirements.

[13] Arizona Supreme Court, *Administrative Order No. 2005-12: Adopting the standardized assessment and reassessment tool and conducting a pilot program for reassessment timeframes for adult intensive probationers.* <http://www.azcourts.gov/portals/22/admorder/orders05/2005-12.pdf> accessed 20 March 2019.

[14] J. Ferguson, 'Putting the "what works" research into practice: An organizational perspective' (2002) 29 Criminal Justice and Behavior 480-481.

[15] ibid 485.

The Risk Level Classifications include the following categories: high violent; high non-violent (drug/property); moderate; low.[16]

Specific risk assessment tools were proposed to be used in Europe following terrorist attacks as a result of discussions which took place in Brussels on 9 and 10 July 2018 on Radicalization Awareness Network - RAN P&P meeting on risk assessment implementation. The risk assessment tools proposed, addressing only terrorism issues were: Radicalization Risk Assessment in Prisons (RRAP) tool set, VERA-2R and ERG 22+. [17]

2. The "Trojan Horse" effect

Risk assessment tools are, as a matter of fact, complex AI systems. How do they actually work? Their outputs were qualified as unpredictable and opaque, due to the fact that specific human rights are to be particularly affected.[18]

It is obvious that their use in the criminal justice system seems proper and the utmost efficient. But, in fact, the use of algorithms may lead to rights violations or may undermine the effective enjoyment of these human rights in the following cases, making them a modern Trojan Horse.[19]

[16] E. K. Drake and R. Barnoski, 'New risk instrument for offenders improves classification decisions' (Document No. 09-03-1201) (Washington State Institute for Public Policy, 2009) <http://www.wsipp.wa.gov/rptfiles/09-03-1201.pdf> accessed 20 March 2019, 2.

[17] European Commission, 'Prison and Probation Working Group (RAN P&P)' <https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/ran-p-and-p> accessed 21 March 2019.

[18] Council of Europe, Committee of Experts on Internet Intermediaries 'Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications' DGI (2017)12 <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> accessed 15 December 2018, 10.

[19]*Trojan horse*, huge hollow wooden horse constructed by the Greeks to gain entrance into Troy during the Trojan War. The horse was built by Epeius, a master carpenter and pugilist. The Greeks, pretending to desert the war, sailed to the nearby island of Tenedos, leaving behind Sinon, who persuaded the Trojans that the horse was an offering to Athena, goddess of war, that would make Troy impregnable. Despite the warnings of Laocoön and Cassandra , the horse was taken inside the city gates. That night Greek warriors emerged from it and opened the gates to let in the returned Greek

2.1. Fair trial

Automated processing techniques and algorithms in crime prevention and the criminal justice system may affect the presumption of innocence and other procedural rights of the defendant. In the present high-risk society, following the terrorist attacks that took place in Europe and U.S., online social media platforms were and are used to identify potential terrorists and to become efficient in the fight against terrorism.[20] They are also used to identify accounts that generate extremist content. From this point of view, we must agree that there are consequences for the freedom of expression, but also for fair trial standards – art. 6 of the ECHR[21] -, notably the presumption of innocence, the right to be informed promptly of the cause and nature of an accusation, the right to a fair hearing and the right to defend oneself in person. Risk assessment tools may contribute, as shown, to prejudicial and discriminatory decision-making.

2.2. Privacy and data protection

Due to the fact that all risk assessment tools are using algorithms in order to collect and sort all sorts of data and images, serious questions

army. The story is told at length in Book II of the Aeneid and is touched upon in the Odyssey. *"Equo ne credite, Teucri. Quiquid id est, timeo Danaos et dona ferentes"("Do not trust the horse, Trojans! Whatever it is, I fear the Greeks, even bringing gifts.")* See J. K. Robertson, *Virgil s Aeneid Book II, with introducton, notes and vocabulary* (The W. J. Cage Company 1893) 2.

[20] Lindsey Andersen, 'Human rights in the Age of Artificial Intelligence' (*Access Now*, 2018) <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf> accessed 12 December 2018, 22.

[21] Article 6 para 1 and 2 of the ECHR: Right to a fair trial:

1.In the determination of his rights and obligations, or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

about breaching right to respect private and family life provided by art. 8 of the ECHR[22], including the right to data protection. "Algorithms are used in online tracking and profiling of individuals whose browsing patterns are recorded by *cookies*. Moreover, behavioural data is processed from smart devices, such as location and other sensor data through apps on mobile devices, raising increasing challenges for privacy and data protection". Scholars emphasized that ML ("machine learning") models were developed that can accurately estimate a person's age, gender, occupation, and marital status just from their cell phone location data. They were also able to predict a person's future location from past history and the location data of friends. [23]

In the same time, everyone could notice that AI is enabling more invasive surveillance tools. The negative impact of AI-powered surveillance would be felt most acutely by the marginalized populations who are disproportionately targeted by security forces. Also, because permanent monitoring of the general population is neither necessary nor proportionate to the goal of public safety or crime prevention, this will lead to the breach of the right to privacy with certainty. [24]

2.3. Non-discrimination

[22] Article 8 of the ECHR: Right to respect for private and family life:

1.Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[23] Steven M. Bellovin, Renée M. Hutchins, Tony Jebara and Sebastian Zimmeck, 'When enough is enough: Location tracking, mosaic theory, and machine learning' (2014) 8 (2) New York University Journal of Law and Liberty <https://digitalcommons.law.umaryland.edu/fac_pubs/1375/> accessed 10 December 2018, 555-556.

[24] Andersen (n 20) 21.

The right to enjoy all human rights and fundamental freedoms without discrimination and in full equality is one of the most important rights in the democratic countries.

In a study prepared for the Council of Europe on algorithms and human rights, it was emphasized that ”search algorithms and search engines by definition do not treat all information equally. While processes used to select and index information may be applied consistently, the search results will typically be ranked according to perceived relevance. Accordingly, different items of information will receive different degrees of visibility depending on which factors are taken into account by the ranking algorithm.”[25]

A biased algorithm that systematically discriminates one group in society, for example based on their age, sexual orientation, race, gender or socio-economic standing, may raise considerable concerns not just in terms of the access to rights of the individual end- users or customers affected by these decisions, but also for society as a whole. Some authors have even suggested that online services which use personalised rating systems are inherently likely to lead to discriminatory practices.[26]

2.4. Equality

In order to develop ML process, the computers must be ”fed” with huge amount of data consisting in texts, images or recordings of sounds (e.g. human voice) – and then adding a classifier to this data (e.g. The computer is shown an image of a woman working in an office and then labelling this as woman office worker. In time the computer will learn to recognise similar images and be able to associate these images with women working in an office and eventually make predictions for things such as job candidate screening or making loan approvals.[27]).

The platform LinkedIn was reported because highly-paid jobs were not displayed as frequently for searches by women as they were for men

[25] Council of Europe, Committee of Experts on Internet Intermediaries (n 18) 26.

[26] Alex Rosenblat and Luke Stark, ‘Algorithmic Labor and Information Asymmetries: A Case Study of Uber’s Drivers’ (2016) 10 International Journal Of Communication <https://ssrn.com/abstract=2686227> accessed 10 December 2018, 3777.

[27] Bettina Büchel, ‘Artificial intelligence could reinforce society’s gender equality problems’ (*The Conversation UK*, 1 March 2018) <http://theconversation.com/artificial-intelligence-could-reinforce-societys-gender-equality-problems-92631> accessed 12 December 2018.

because of the way its algorithms were written. And the algorithms were written that way because, in the beginning, man users of LinkedIn were predominantly looking for the high-paying jobs, so the ML ended up proposing these jobs to men – thus discriminating women and reinforcing the bias against them[28].

Also, automated testing and analysis of Google's advertising system reveals male job seekers are shown far more adverts for high-paying executive jobs.[29]

Another research has showed that two prominent research-image collections—including one supported by Microsoft and Facebook—display a predictable gender bias in their depiction of activities such as cooking and sports. Images of shopping and washing are linked to women, for example, while coaching and shooting are tied to men.[30] If a photo set generally associates women with housework, softwares trained by studying those photos and their labels create an even stronger association with it.[31]

The criminal justice system, increasingly relying on risk assessment tools as showed before, makes no exception on the discrimination issue and the breach of equality between citizens, being qualified as "in crisis"[32]. Studies have revealed "persistent racial disparities at every stage, a different kind of justice for the haves and the have nots, and a system that neither rehabilitates individuals nor ensures public safety"[33].

When person is arrested in U.S. for example, he or she will be usually subjected to a pre-trial risk assessment tool in order to help the judge

[28] Hope Reese, 'Bias in machine learning, and how to stop it' (*TechRepublic*, 18 November 2016) <https://www.techrepublic.com/article/bias-in-machine-learning-and-how-to-stop-it/> accessed 10 December 2018.

[29] Samuel Gibbs, 'Women less likely to be shown ads for high-paid jobs on Google, study shows' (*The Guardian*, 8 July 2015) <https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study> accessed 12 December 2018.

[30] Tom Simonite, 'Machines Taught by Photos Learn a Sexist View of Women' (*Wired*, 21 August 2017) <https://www.wired.com/story/machines-taught-by-photos-learn-a-sexist-view-of-women/> accessed 10 December 2018.

[31] Büchel (n 27).

[32] Vincent Southerland, 'With AI and Criminal Justice, the Devil is in the Data' (*ACLU*, 9 April 2018) <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/ai-and-criminal-justice-devil-data> accessed 15 December 2018.

[33] ibid.

decide whether to incarcerate that person pending trial or to release that person. Some U.S. states have used these pre-trial AI tools at the sentencing and parole decision stage, in an attempt to predict the likelihood that someone will commit a new offense if released from prison[34].

But the negative consequences of this use are serious because of the biases they reinforce and perpetuate. Because all risk assessment tools are based on actuarial historical data, if the data is not accurate or is obtained due to some illegal or exaggerate conduct (e.g. policemen in a city are usually arresting people from a certain community in a period of time. If that data is fed to the computer, the predictive model will suggest that people from that community are generally more likely to commit crimes so the results of the predictive test will perpetuate the discriminating pattern). If the algorithms are not ”cleaned” of the waste (discriminatory patterns), the use of such AI tools will produce more harm than benefit for the justice system.

A study revealed that Black defendants were more likely to be wrongly labelled high risk than white defendants drawing attention on the perils of risk assessment tools ”scoring”.[35] In many of the US states, ”the results of such assessments are given to judges during criminal sentencing. Rating a defendant’s risk of future crime is often done in conjunction with an evaluation of a defendant’s rehabilitation needs. The Justice Department’s National Institute of Corrections now encourages the use of such combined assessments at every stage of the criminal justice process.”[36]

The study revealed that only 20 percent of the people predicted to commit violent crimes actually reiterated their criminal conduct. Also, in forecasting who would re-offend, the algorithm made mistakes with African-American and white defendants at roughly the same rate but in very different ways. The formula was particularly likely to falsely flag black defendants as future criminals, wrongly labelling them this way at almost

[34] ibid.

[35] Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, ‘Machine Bias. There’s software used across the country to predict future criminals. And it’s biased against blacks’ (*ProPublica*, 23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 12 December 2018.

[36] ibid.

twice the rate as white defendants. White defendants were mislabelled as low risk more often than black defendants.[37] As a matter of fact, 23,5% of white people were labelled higher risk, but didn't re-offend in opposition with 44,9% African-American. In the same time 47.7% of white defendants were mislabelled as lower risk, yet DID re-offend, while 28.0% African-American labelled lower risk actually reiterated their criminal conduct.[38]

3. Concluding remarks

In spite of all benefits resulted in using risk assessment tools, there are still a lot of issues the scholars and practicioners must address. Fiew initiatives, such as the adoption of Toronto Declaration[39] or prudent approach by the Courts[40] are not quite enough to determine what long-term effects the widespread use of such artificial tools is going to produce.

Accepting these new instruments in the criminal justice field in a hurry and with great joy is going to transform the criminal justice system in an area of impredactibility and false objectiviy. As shown in Chapter 2 of the present study, the objective outcomes are in fact sources of discrimination and violetions of the elementary human rights guaranteed bu ECHR. My persopnal recommendation is to approach the issue with

[37] Angwin et al. (n 35).

[38] ibid.

[39] Fulltext of Toronto Declaration available at <https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf> accessed 12 December 2018.

[40] See *State v. Loomis,* 881 N.W.2d. (Wisc. 2016). This case was one of the first major cases to address concerns about whether a judge's consideration of a software-generated risk assessment score during sentencing constitutes a violation of due process or overt discrimination. The Loomis case, challenged the use of COMPAS as a violation of the defendant's due process rights. But the Wisconsin Supreme Court held that Loomis's challenge did not clear the constitutional hurdles. Importantly, the case relies on two prior state court decisions: *State v. Samsa (*2015 WI App 6) and *State v. Skaff* 447 N.W.2d 84, 85 (Wis. Ct. App. 1989), the last one a 1989 decision which held that the right to be sentenced based on accurate information includes the right to review and verify information contained in the pre-sentence investigation report. As a matter of fact one of the most important arguments in the court's reasoning in the Loomis case was the fact that the COMPAS score cannot be the only thing the sentence is based on, or even the determinative factor, thereby arguably ensuring that the judge will consider other information about the particular case and assign an individual sentence based on the totality of the circumstances.

caution and to rely on such instruments in the criminal justice field only to strenghten the decision of the Courts and not to ground it.

References

- Andersen, Lindsey, 'Human rights in the Age of Artificial Intelligence' (*Access Now*, 2018) <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf> accessed 12 December 2018
- Angwin, Julia; Larson, Jeff; Mattu, Surya and Kirchner, Lauren, 'Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks' (*ProPublica*, 23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 12 December 2018
- Arizona Supreme Court, *Administrative Order No. 2005-12: Adopting the standardized assessment and reassessment tool and conducting a pilot program for reassessment timeframes for adult intensive probationers.* <http://www.azcourts.gov/portals/22/admorder/orders05/2005-12.pdf> accessed 20 March 2019
- Bellovin, Steven M.; Hutchins, Renée M.; Jebara, Tony and Zimmeck, Sebastian, 'When enough is enough: Location tracking, mosaic theory, and machine learning' (2014) 8 (2) New York University Journal of Law and Liberty <https://digitalcommons.law.umaryland.edu/fac_pubs/1375/> accessed 10 December 2018
- Brennan, T.; Dieterich, W. and Ehret, B., 'Evaluating the Predictive Validity of the Compas Risk and Needs Assessment System' (2009) 36 Criminal Justice and Behavior <DOI: 10.1177/0093854808326545> accessed 18 March 2019
- Büchel, Bettina, 'Artificial intelligence could reinforce society's gender equality problems' (*The Conversation UK*, 1 March 2018) <http://theconversation.com/artificial-intelligence-could-reinforce-societys-gender-equality-problems-92631> accessed 12 December 2018

- Council of Europe, Committee of Experts on Internet Intermediaries 'Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications' DGI (2017)12 <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> accessed 15 December 2018
- Desmarais, S. L.; Johnson, K. L. and Singh, J. P., 'Performance of Recidivism Risk Assessment Instruments in U.S. Correctional Settings' (2016) 13 (3) Psychological Services
- Drake, E. K. and Barnoski, R., 'New risk instrument for offenders improves classification decisions' (Document No. 09-03-1201) (Washington State Institute for Public Policy, 2009) <http://www.wsipp.wa.gov/rptfiles/09-03-1201.pdf> accessed 20 March 2019
- European Commission, 'Prison and Probation Working Group (RAN P&P)' <https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/ran-p-and-p> accessed 21 March 2019
- Ferguson, J., 'Putting the "what works" research into practice: An organizational perspective' (2002) 29 Criminal Justice and Behavior 472-492
- Gendreau, P.; Little, T. and Goggin, C., 'A meta-analysis of the predictors of adult offender recidivism: What works!' (1996) 34 Criminology 575-608 <doi: 10.1111/j.1745-9125.1996.tb01220.x> accessed 10 March 2019
- Gibbs, Samuel, 'Women less likely to be shown ads for high-paid jobs on Google, study shows' (*The Guardian*, 8 July 2015) <https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study> accessed 12 December 2018
- Kehl, D.; Guo, P. and Kessler, S., 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative' (*Berkman Klein Center for Internet & Society, Harvard Law School*, 2017) <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041> accessed 10 May 2019
- Latessa, E.; Smith, P.; Lemke, R.; Makarios, M. and Lowenkamp, C., 'Creation and validation of the Ohio Risk Assessment System:

Final report' (2009) <https://www.assessments.com/> accessed 20 March 2019

– Matacic, C., 'In the United States, computers help decide who goes to jail. But their judgment may be no better than ours' (*Science*, 17 January 2018), <https://www.sciencemag.org> accessed 18 March 2019

– Miller, H. A., 'A Dynamic Assessment of Offender Risk, Needs, and Strengths in a Sample of Pre-release General Offenders' (2006) 24 Behavioral Sciences and the Law 767–782 <https://onlinelibrary.wiley.com/doi/abs/10.1002/bsl.728> accessed 20 March 2018

– Raynor, P.; Kynch, J.; Roberts, C. and Merrington, S., 'Risk and need assessment in probation services: an evaluation' (2000) 211 Home Office Research Study <https://www.researchgate.net/publication/267419138_Risk_and_Need_Assessment_in_Probation_Services_An_Evaluation/download> accessed 12 December 2018

– Reese, Hope, 'Bias in machine learning, and how to stop it' (*TechRepublic*, 18 November 2016) <https://www.techrepublic.com/article/bias-in-machine-learning-and-how-to-stop-it/> accessed 10 December 2018

– Robertson, J. K., *Virgil s Aeneid Book II, with introducton, notes and vocabulary* (The W. J. Cage Company 1893)

– Rosenblat, Alex and Stark, Luke, 'Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers' (2016) 10 International Journal Of Communication <https://ssrn.com/abstract=2686227> accessed 10 December 2018

– Simonite, Tom, 'Machines Taught by Photos Learn a Sexist View of Women' (*Wired*, 21 August 2017) <https://www.wired.com/story/machines-taught-by-photos-learn-a-sexist-view-of-women/> accessed 10 December 2018

– Southerland, Vincent, 'With AI and Criminal Justice, the Devil is in the Data' (*ACLU*, 9 April 2018) <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/ai-and-criminal-justice-devil-data> accessed 15 December 2018

– Toronto Declaration available at <https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf> accessed 12 December 2018

Short biography of the author

Mrs. Laura Stanila PhD, is Senior Lecturer at the Faculty of Law, West University Timișoara, Romania. Her 20-year-long teaching expertise and research include Criminal Law and Sociology of Law, over 70 articles, studies and bookchapters published in international and Romanian Journals, 9 books and one national prize in 2012 (*"Ion Tanoviceanu" Prize* in 2012 awarded by Romanian Jurists Union for the monography *Răspunderea penală a persoanei fizice [Criminal Liability of the natural person]*). In 2015 Mrs. Stănilă has completed a post-doctoral research on Bioethics and Criminal Law and written a very well received monography *Provocările Bioeticii și răspunderea penală [Challenges of Bioethics an Criminal Liability]*. She also is a member of an impressive number of professional associations (e.g. Romanian Asociation of Penal Sciences, International Assosiation of Criminal Law, Jurists Union of Romania, Victimology Society of Serbia etc.) as well as member in several Boards of Editors of prestigious national and international Journals (e.g."Analele Universității de Vest Timișoara Seria Drept, "Journal of Eastern European Criminal Law", "OJLS- Open Journal for Legal Studies", etc.).

II. Cryptocurrencies

Central bank issued digital currencies: is it a solution or a problem?

Zsolt Bujtár*

Abstract: Central bank issued digital currencies (CBDC) can be the viable substitutes of current cash and account type money. It is a major change any central bank should be careful about when introducing. The author examines the causes behind the urgency of introduction. One major driving force behind near future introduction can be the competition stemming from the launch of Libra, Facebook's new digital money as a payment tool. It is also discussed in the paper how and with what kind of drawbacks and advantages can a new digital money be part of the monetary toolset of central banks.

Keywords: CBDC, monetary policy, digital money

1. Introduction

Central bank issued digital currencies (CBDC) are in the focus of more than 60 % of the central banks, representing 80 % of the population all around the world.[1] Central banks have taken under scrutiny the possibilities of introducing a CBDC, and global financial institutions like the World Bank even experiment with a pseudo CBDC.[2] Certain smaller countries tried to pioneer the process, but failed to achieve even short-term successes (Marshall Islands, Ecuador). China has also announced the creation of a new public CBDC, but has given no details about the date

* Assistant lecturer, University of Pécs, Faculty of Law, Department of Business and Commercial Law, bujtar.zsolt@ajk.pte.hu.

[1] Augustín Carstens, 'The future of money and payments: Speech by Mr Agustín Carstens, General Manager of the BIS, at the Central Bank of Ireland, 2019 Whitaker Lecture, Dublin, 22 March 2019' <https://www.bis.org/speeches/sp190322.htm> accessed 21 July 2019.

[2] Ana Berman, 'IMF and World Bank Launch Quasi-Cryptocurrency in Exploration of Blockchain Tech' (*Cointelegraph*, 14 April 2019) <https://cointelegraph.com/news/imf-and-world-bank-launch-quasi-cryptocurrency-in-exploration-of-blockchain-tech?fbclid=IwAR2hrCpg42VOM7Wl4jwFL5TSk57tWIDJog8NO5tB2g0S8Fc5uBOe8qL039k> accessed 1 August 2019.

of introduction and specifics of new money.[3] It is a quite complex challenge to introduce a new money when doing so is not an urgent public necessity like in the case of hyperinflation. This is why such a decision in the future should be planned and executed carefully.

Why is it so abruptly urgent to evaluate such a major overhaul in the financial system? There are several reasons, but at least three of them are worth examining: the first is technological development, the second is the appearance of major competitors like Facebook, while the third encompasses the numerous advantages a new monetary tool can offer. On the other hand, there are also certain drawbacks which make the decision-making process regarding the introduction of CBDC even more complex.

In this study, the author examines the major advantages and disadvantages of the possible introduction of different types of central bank issued digital moneys.

After defining the different types of money, CBDCs and their functions, the author examines the functions of fiat money versus digital money. The paper assesses Libra, Facebook's new world money in a separate section. Finally, the advantages and drawbacks of different forms of CBDC usage are presented, examined as digital money and a potential tool of monetary policy.

2. CBDC defined - Central bank issued digital currencies

To provide the definition of central bank issued digital currency, it is necessary to classify the types of money and its equivalents currently in use as well as certain new forms of money.

Taxonomy of money by its basic functions differentiated between several distinct categories. In the latest IMF research paper of July 2019,[4] experts set up a money tree-like table, which classifies the differences of

[3] Thomas Simms, 'China's Digital Currency Is Ready, Central Bank Says' (*Cointelegraph*, 11 August 2019) <https://cointelegraph.com/news/chinas-digital-currency-is-ready-central-bank-says> accessed 12 August 2019.

[4] Tobias Adrian and Tommaso Mancini-Griffoli, 'The Rise of Digital Money' (July 2019) International Monetary Fund Fintech Note/19/1 < https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>.

money with four characteristics.[5] According to the model, these characteristics are: type, value, backstop and technology. The IBS Committee on Markets and Payment Infrastructure in 2018 set up a taxonomy called money flower, in which money is classified on the basis of issuer, form, accessibility and technology.[6] In the latter, widely spread IBS model form types divide public/retail CBDC[7] into token and account type. The problem in the IBS model with using token and account types is that cryptocurrencies are divided into several token types like investment, utility and its hybrid, etc.[8] As a result, this classification can be confusing, since a potential digital CBDC - as we will see later - can be at least theoretically DLT-typed[9], just like cryptocurrencies.

Based on the above-mentioned fact, the author uses the IMF money tree model in this study. There are two main categories of money type according to IMF money trees, which are the following: claim and object. The claim is defined as a liability of an entity not being present. This also means that paying by a claim type money can be instant, but the actual delivery of the money occurs later. In the meantime, an amount is deposited as a collateral of the actual payment, made by the claim, until the actual payment is made.

Claims have two forms, according to their redemptions value: fixed value or valuable redemption value. Fixed value redemptions are divided into two subcategories: b-money and e-money. B-money has a final guarantee in case its obligator is not able to fulfil its obligation. This so-called backstop can be either a deposit insurance scheme or a central

[5] Bank for International Settlements: Committee on Markets and Payment Infrastructure, Market Committee, 'Central bank digital currencies' (March, 2018) <https://www.bis.org/cpmi/publ/d174.pdf>.

[6] ibid 4-6.

[7] Public or retail CBDC, a digital money, is available for public use similar to cash nowadays, contrary to wholesale CBDC, which is available for legible financial institutions only.

[8] Gábor Szalay, 'A kriptovaluták nemzetközi szabályozási trendjei: Kriptotőzsdék és ICO-k értékpapírjogi perspektívából' (2019) 74 (3) Jogtudományi Közlöny 126-134.

[9] Distributed ledger technology (DLT) has a basic feature, which differentiates it from other centralized data processing and storage systems. DLT uses a web of computers, which has to agree on adding new data to a bloc of data. The owners of these computers are independent from each other, and their functioning is based on a predetermined consensus of proof of work or proof of stake.

bank's action, called lender of last resort.[10] In both cases[11] the central bank has unlimited power and the obligation to maintain the public's trust placed in the monetary system. These monies are either direct claims towards a bank account (debit card) during an instant payment cleared later, or indirect claims for risk-free securities like government bonds of different states - in case of money market funds. National settlement systems of commercial banks are also part of the b-money group in a country, where these settlements are supervised or even executed by the central bank of a given state.[12] It is important to note these settlements since they are forms of digital currency, and as such they are the potential predecessors of public/retail CBDC.

Contrary to b-money, e-money is issued by a private entity that uses either a centralized or a decentralized technology, which controls issuance and clearance of this type. As its name implies, e-money is only a settlement money, there is no possibility to transfer this claim into cash form. It only functions as a money to buy services or goods provided by its issuer (actually its operator, since there is no money issued as it is only a privilege of central banks) or its subcontractor. Clearance can be made instantly if using card service companies like Visa or Mastercard, but usually it takes more time. The main characteristic of e-money is that it is only an online platform with payment services operated through the internet. Since it is only an agent type activity, the actual settlement made in b-money, which makes this money payment a fix-value-redemption type too, is similar to b-money transactions.

Claim type money has a special subtype called l-money, which is a variable-value redemption. Its variability (actually volatility) stems from the fact that its issuer is not a central bank and is not backed by one currency

[10] Lender of Last Resort (LOLR) is a key role for the monetary system. The central bank in a two-tier bank system or in the case of a one-tier bank system is a dedicated financial institution having the exclusive right to exercise this function. When a commercial bank needs emergency liquidity in case of a bank run, with certain conditions the central bank can provide unlimited cash to stop the fear of the bank running out of necessary cash to pay depositors.

[11] Deposit insurance system has limited money mostly from compulsory membership payments. If it is not enough to cover depositors' losses, money is lent to the deposit insurance agency though security issuance guaranteed by the state.

[12] A good example is the Real Time Gross Settlement System (RTSG) see Michael Kumhof and Clare Noone, 'Central Bank Digital Currencies - Design Principles and Balance Sheet Implications' (2018) Bank of England Working paper No. 725, 3.

like for example currency backed stablecoins. Stablecoins are cryptocurrencies - among them the most notorious is tether[13] - which claim or actually back its cryptocurrency by low volatility assets, like gold or fiat currency (as it is claimed by tether founders by USD), or basket of fiat currency like Libra. In such situations, I-money is a claim that cannot be transferred fully to fiat currency without price fluctuation, since its fiat currency conversion depends on the price of the asset it is backed by.

The difference between decentralized, privately issued e-money like Paxos and I-money type Libra has significant importance with respect to this study. The fine line of difference is based on who issues the same basic type of money, like in the case of cryptocurrencies. Paxos, for example, is a stablecoin issued by a New York State licensed financial institution, a trust company[14], whilst Libra's will be issued by an association based in Switzerland in which Facebook has only USD 10 million stake out of a USD 1 billion capital. Because of the above-mentioned facts, Paxos is a centralized stablecoin while Libra is decentralized. Libra's value can fluctuate according to the fiat currency basket against which it is defined, but Paxos guarantees to change Paxos tokens[15] to USD on its crypto exchange itBit and also on the over-the-counter market for Paxos (PAX OTC) with a 7/24 availability.[16]

In the case of an object as money, not only the payment is instant, but the transfer of money as a unit of account as well. There is no need for future clearance, since cash changes hand on the spot, finishing the transfer of money transaction too (not only the change of goods or services). This is the case for paper money or coins. It can be similar in the case of a central bank issued digital currency, when it is issued as a token on a digital device like mobile phones or tablets. As it is assessed in this paper, both type of CBDCs can be issued by the given central bank

[13] Tether real full USD backing was questioned several times, see Nikhilesh De, 'Tether Lawyer Admits Stablecoin Now 74% Backed by Cash and Equivalents' <https://www.coindesk.com/tether-lawyer-confirms-stablecoin-74-percent-backed-by-cash-and-equivalents> accessed 12 June 2019.

[14] Charles Cascarilla, 'Paxos standard white paper' (2018) <https://www.paxos.com/wp-content/uploads/2019/02/PAX_Whitepaper.pdf> accessed 22 July 2019

[15] ibid.

[16] ibid.

or any institution having a mandate from a central bank, but in the latter case only as a decentralized CBDC.

This differentiation of centralization will have its relevance later when CBDC is examined as a monetary policy tool. CBDC in both cases works as a unit of account, meaning that it can be a measurement of goods and services. In case of cryptocurrencies issued by independent entities like bitcoin[17] or ether, it has no unit of account function as long as it has the enormous volatility like bitcoin or ether have since their inception.[18]

The borderline between the five different money types is not finite. E-money issued in a digital form by private entities as money market funds' shares or ETFs can easily become I-money, when its shares are tokenized or issued as coin representing certain unit of share in a money market fund or an ETF in any digital ledger. This is possible because traditional mutual funds and ETFs – as shadow banking entities – overgrew the traditional banking system.[19]

For the complete summary of different functions along four classifications of monies see Figure 1 below.

[17] Bitcoin has no independent entity which issues new bitcoins. It is mined by solving computer algorithms for which miners get bitcoins as a reward. Bitcoin has a limited number to be issued 21 000 450.

[18] The other major concern with cryptocurrencies is their limited regulation (to certain jurisdictions like Malta or Switzerland), if any at all. See Zsolt Bujtár, 'A kriptovaluták európai és máltai szabályozásának összehasonlítása: A máltai sólyom szárnyalása' (2018) 18 (5) Európai Jog 6-16 and András Kecskés and Zsolt Bujtár, 'A kriptovaluta ökoszisztéma európai uniós és a svájci szabályozásának összehasonlítása' (2018) 24 (2) JURA 427-439.

[19] Adrian and Mancini-Griffoli (n 4).

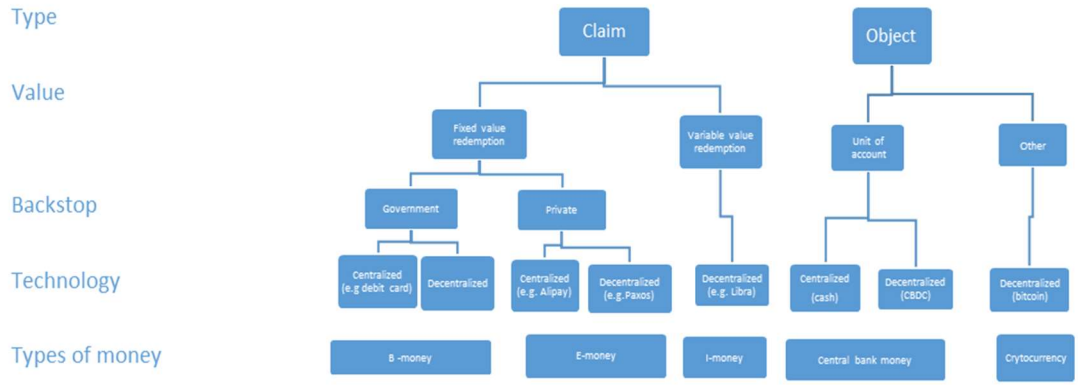


Figure 1: Money trees[20]

3. CBDC potential types and their functions

Central bank money in its early form already existed as a unit of account in central settlements between commercial banks and their central bank. (See RTSG above as an example.) This is because this type of money is not printed in any cash form, it exists only as the net or gross claims of banks against each other to have a daily settlement, which amount should actually be paid by the one who has net liability towards the one who has net claim. However, this central bank issued money is not DLT type like cryptocurrency, but it is data as an electronic settlement input. CBDC can be DLT type as well, like cryptocurrencies, or based on other technology that makes it digitally possible to issue, store, retrieve digital money supervised by a central bank.

The difference between central bank issued centralized CBDC and decentralized CBDC is the one who operates the technology that creates (mines or controls and sets up smart contract) the CBDC. In the case of centralized CBDC, creation is fully controlled by a central bank. However, in the case of decentralized CBDC, a central bank gives up its full control

[20] Adrian and Mancini-Griffoli (n 4).

of creating money by giving the right to a third party – let it be a private or public, or non-profit entity – to mine or create in other way (e.g. by a smart contract) CBDC. It is relevant whether it is a centralized or a decentralized CBDC, since issuing money is the monopoly of central banks, as a central bank's control of the money supply forms an integral part of its monetary policy. Because of this, central banks hardly even support the idea of issuing money which is uncontrolled in its quantity by the given central bank having jurisdiction over monetary policy under the laws of a given state.

The question is the following: why would a central bank replace a fiat money or support a parallel money besides its own fiat money. From the perspective of the banking system, the negative interest rate policy is one major reason. Because in case of a new CBDC, which is a different money type than fiat, the central bank can pay different interest on CBDC deposits. On CBDC deposit this can also be negative interest on the long run, but on fiat money it should be positive to attract savings for the financial institutions to finance loans and to remain profitable. The other important issue is wholesale and retail money differentiation. Wholesale money, which is already a digital money, is a type of money that is used in interbank systems by privileged financial institutions.[21] Retail CBDC is one that would be available for households and nonfinancial institutions too. If only the wholesale financial actors could use it with the functions above, then it would not be a new digital money, but only the acknowledgement of the status quo. In the following part, the author examines the possible advantages of the two above-mentioned types of CBDC.

4. Public/retail CBDC – can it be a reality?

Public/retail CBDC is a time journey in terms of going back to a certain level, to the one-tiered banking system, in which all economic actors except for households could have an account at the central bank. Already in 1987, the one-tiered banking system ceased to exist in Hungary. The possible difference is that even to households, access to new CBDC has

[21] As an example, in Switzerland roughly 200 financial institutions. See Aleksander Berentsen and Fabian Schar, 'The Case for Central Bank Electronic Money and the Non-Case for Central Bank Cryptocurrencies' Review, Federal Reserve Bank of St. Louis (2018) 100 (2).

to be given. But the household cannot be defined as an account holder, only the persons within the household, i.e. the citizens. Citizens in the free world, however, can move abroad or keep a citizenship and get another one, if the home country – based on its laws – so allows. This leads to the private persons' taxation problems. Several hundreds of thousands change citizenship or settle in a low tax bracket country in order to pay less or no personal income or corporate tax. This is especially true in the case of countries which are considered as tax havens and take bank privacy seriously. The central banks of these countries have to draw a line when determining who can open a CBDC account. For example, Switzerland or Cyprus can attract foreigners to open CBDC accounts at their respective central banks.

This is possible because CBDC can replace current cash money, as it can work as an emergency reserve during problematic events like bank-runs (in 2008 during the subprime mortgage crisis of 2007-2009) or state bankruptcy (for example in Venezuela in 2018-2019, or in Argentina and Ukraine numerous times in the last 50 years). Cash is problematic because of its anonymity. It can be used for money laundering and tax evasion as well. This is why it can be another incentive for a central bank to replace it with CBDC or minimize its usage by the parallel usage of CBDC. The question is why a private person would change cash for CBDC. And the answer is: because of the reputation of central banks. Contrary to commercial banks, modern central banks have a reputation of providing sufficient trust for the public to hold their money at the given central bank, just like cash at home. Central banks earned this reputation by playing the lender of last resort role during the previous century when the financial system collapsed as a result of the Great world Crisis of 1929-1933 and the Great Financial Crisis of 2007-2009. The FED,[22] the US central bank, rescued not only the commercial banks as part of the US program named

[22] Programs for shadow banking actors were Commercial Paper Funding Facility (CPFF), Asset-Backed Commercial Paper Money Market Mutual Fund Liquidity Facility (AMLF), Money Market Investor Funding Facility (MMIFF), and the Term Asset-Backed Securities Loan Facility (TALF) <https://www.federalreserve.gov/monetarypolicy/bst_crisisresponse.htm> accessed 21 July 2019.

TARP, [23] but also insurance companies like AIG or complete financial sectors like the money market mutual funds.[24] The latter financial institutions, however, were not the part of deposit insurance schemes, but of a new phenomenon called the shadow banking system.[25]

In that case, a possible solution can be the introduction of CBDC to avoid the next great crisis which has already been dubbed - although it has only early indications – as the Great Liquidity Crisis, which is mainly the result of central banks' quantitative and qualitative easing policies. As the next crisis arrives, there are two possible solutions to keep the world economy and the financial system afloat: one is the Chicago Plan[26] and the other is helicopter money.[27] Professor Henry Simons from the University of Chicago coined the Chicago plan in 1936. According to his theory, commercial banks have to keep 100 % reserve on deposits by government-issued money. There are four benefits of this potential new financial system besides not causing another financial crisis. These four advantages are: commercial banks cannot create money and thus credit, which allows much easier control of credit cycles, furthermore, it would eliminate bank runs, while the central bank could issue money at zero

[23] TARP - Troubled Asset Relief Program, as part of Emergency Economic Stabilization Act of 2008 provided much needed liquidity for the financial system by buying securitized obligations.

[24] Gábor Szalay, 'The Impact of the Lack of Transparency on Corporate Governance: A Practical Example' (2018) 1 (2) Corporate Law & Governance Review 21-28 <www.virtusinterpress.org/IMG/pdf/clgrv1i2p2.pdf> accesssed 12 July 2019.

[25] Shadow banking system is a part of the financial system like traditional banking system conduct maturity, liquidity and risk transformation without deposit insurance schemes and lender of last resort central bank as a backstop for investors. That is why a shadow bank run can be so dangerous as a bank run, but even more risky for the financial system. That is why as an exception the FED intervened to rescue some shadow banking institutions to avoid the collapse of the whole financial system. András Kecskés and Zsolt Bujtár, 'Az árnyékbankrendszer jogi szabályozása az Egyesült Államokban és az Európai Unióban' (2017) 23 (1) JURA 266-277.

[26] Jaromir Benes and Michael Kumhof, 'The Chicago Plan Revisited IMF Working Paper August 2012' <https://www.imf.org/external/pubs/ft/wp/2012/wp12202.pdf> accessed 22 July 2019.

[27] Helicopter money's definition was introduced by Milton Friedman in 1969, but was popularized in 1986 by former FED Chairman Ben Bernanke in 2002. According to theory central bank can inject money into the economy to exert inflation or increase GDP. It can be a one-time or a permanent policy action as well. Ansgar Belke, 'After the Bazooka a Bonanza from Heaven – „Helicopter Money" Now?' (2018) ROME Discussion Paper Series, No. 18-02.

interest rate, and finally private and public debt would reach much lower levels. Both the helicopter money and the Chicago plan have advantages and disadvantages, but both has reputational risk[28] for a central bank to introduce. However, if with respect to both above-mentioned scenarios - against all the advantages - hyperinflation occurs, the trust in the financial system and especially in central banks will be lost.

This can also happen in the case of CBDC. If public trust would be lost due to hacking attacks[29] in connection with a CBDC, the central bank would suffer a reputation loss, the risk of which is not worth taking by central banks as institutions, being responsible for price stability and the stability of the financial system.

5. CBDC as a monetary policy tool

Current financial systems with the use of fiat money have one monetary system with the only type of money as a legal tender. All money on international money markets are treated as equal, meaning that any currency, cash or reserve, can be converted easily if freely floated. At the same time, reserve money can have a very different interest as opposed to the same money invested as private money in the form of government bonds. As an extreme example in Hungary, a commercial bank reserve has negative interest, but a new premium government bond pays on average 4,94 % interest fixed for five years.[30] The example shows how money can transform from one form to another as part of a monetary transmission process.[31] Just days before the introduction of the new government bond the overnight BUBOR rate more than quadrupled. In a weak it normalized, getting very close to the previous level of 0,1 %, but

[28] Benes and Kumhof (n 26).

[29] Szilád Benk, László Kajdi, András Kollarik, Zoltán Mamira, Miklós Szebeny, Gergő Török and Lóránt Varga, 'Digitalizáció és pénzrendszer' Gergely Fábián and Barnabás Virág (eds), *Bankok a történelemben: innovációk és válságok* (Magyar Nemzeti Bank 2018) 696.

[30] <https://alapblog.hu/az-akk-megkavarta-az-mnb-allovizet/> accessed 29 July 2019.

[31] Monetary transmission has four channels bank rates is only one of four. The other three are exchange rate, asset prices capital market and, money credit market, see <https://www.ecb.europa.eu/mopo/intro/transmission/html/index.en.html> accessed 12 June 2019.

with longer maturity BUBOR[32] has increased constantly from 0,15-0,20 to 0,20-0,3 levels.[33]

By the introduction of CBDC there are two possible solutions. One is the introduction of a limited access or wholesale CBDC. This CBDC can only be used by privileged financial institutions having the right to deposit money and certain low risk securities to get money in exchange from the central bank (swap deal) or as a collateral in a repurchase agreement with the central bank. The introduction of this type of CBDC has the advantage of making it feasible to pay higher interest to commercial banks on commercial bank fiat reserves, and making them profitable without changing the reserve money interest as part of the interest monetary mechanism of central banks' monetary policy. This is not much of a difference compared to the current digital money used in the settlement systems of commercial banks. The only difference is maturity; since settlements are made on a daily basis, interest is not relevant on current digital money. As it can have longer than one-day maturity, it can have much lower negative interest relative to fiat money interest rate. This can be a major advantage of this type of CBDC. Since insulated from private companies and private individuals, in the event of a bank run a CBDC would not attract too much liability against the central bank thus the devaluation of current fiat money could not occur.

With respect to public/retail CBDC, there are several problems to be solved. First of all, the above-mentioned negative effect of CBDC on parallel fiat money. Secondly, the central bank's control of money in circulation would become difficult by introducing this type of CBDC. The above-mentioned different interest-system cannot work with a public/retail CBDC because of its usage, as one entity in different channels of monetary transmission is not possible. However, it has to be kept in mind that a major advantage of introducing public/retail CBDC is that it evokes a higher degree of competition between commercial banks compared to a fiat money system. Public/retail money availability can be limited to non-privileged economic actors if this competition-evoking effect (concerning commercial banks) is ruled out from the system, since private individuals or companies in such case could only have CBDC as

[32] BUBOR is abbreviation of Budapest offered bank rate at which commercial banks and Hungarian Central Bank give loans to each other.

[33] <https://www.mnb.hu/monetaris-politika/penzpiaci-informaciok/referenciamutato-jegyzesi-bizottsag/bubor> accessed 29 July 2019.

emergency money, like cash held at home or at home cashiers by companies. Before the author examines the kind of digital money a new CBDC should be, it is worth looking at a major challenge of current fiat money Libra, Facebook's new invention.

6. Libra as a turning point for digital currencies

In the case of a cryptocurrency, the best starting point for analyzing the given asset is examining its white paper. The white paper, as an equivalent of the prospectus in an initial public offering, can give us details about the issuer of the cryptocurrency and its intent, as well as the solution the asset provides for the problem described in the white paper.

Libra's white paper states that its cryptocurrency can solve problems of hundreds of millions of people by providing a cheap and fast payment system for the ones most in need and having no access to commercial banks. This goal is achieved by a blockchain-based stablecoin. In this case, blockchain-based means that it is a DLT type, and as a result all transactions are kept in a distributed ledger verifying each transfer by different computer nodes. In the case of Libra, a basket of currencies weighted means all fiat money invested in short term government securities issued by reputable central banks as a collateral for Libra. There will be no hedging of reserves, thus the value of Libra will only change if its basket currencies change.

The question arises why the 2020 introduction of Libra became such an important event in the summer of 2019. There are two reasons: the first is Facebook's more than 2.2 billion users, who are all potential clients of Libra payment methods, while the second is that if it succeeds it can pose a danger for the current role of USA dollar as a world currency. This is why almost all major financial authorities have raised their concerns against the fast introduction of Libra. Major criticism came from traditional commercial banks, being afraid of losing payment revenues and receiving a new competitor having completely different rules with respect to know your customer (KYC) rules working against anti-money laundering (AML) activities. With respect to introducing CBDC as a new digital money, a possible success of Libra known to billions of people would be a major catalyst. With the possible success of Libra, digital money can become a household asset, and the introduction of a CBDC would be viable if other conditions are also met.

Let us assume that Libra will be successful in early 2020. In that case, central banks can start working on a digital currency issued to the public, but in a limited amount of value and to locals only. This is the answer for the question raised at the end of the previous chapter: which type of CBDC should central banks issue? The central banks having the greatest need for new tools for fighting deflation and possessing very few tools since being in a negative interest rate environment like Japan, Sweden or Switzerland, also including the Eurozone. Although DLT technology is very attractive, the safety thereof is not proven 100 %. This is the underlying reason why the author agrees with professor Berentsen and his fellow researcher Fabian Schar on not risking central banks' reputation by using a DLT technology for a CBDC which has not proved its security at the highest level, but rather with one having high security, scalability.

7. Conclusions

As the author examined the possible introduction of central bank issued digital currencies, it can be concluded that it is a very complex problem to solve. The clock is ticking, while the launch of a potential digital money, a DLT type having the capability to be a new world currency (Libra) is already on the horizon. As wholesale digital money is already introduced de facto into money markets for privileged financial institutions only, a public digital money controlled by central banks can be the new type of CBDC. This is the one considered by central banks to be introduced. Fiat money as legal tender has not only object form as cash, but as b-money as claim or e-money as well. Central banks have the responsibility to keep the monetary system not only liquid, but also to keep its operation sustainable. Central banks use different forms of money to coordinate monetary policy in four different channels, and almost all of them with international relationships. By changing fiat money to digital money for the public, this transmission process is also overhauled. Bank runs and shadow bank runs are ruled out by definition, but new problems like cyberattacks arise. Most of the central banks consider it necessary to evaluate the introduction of a new money in the form of CBDC, however, as a conclusion, it can be stated that such introduction should be well prepared, gradual and limited at first, if it becomes necessary at all. According to our current knowledge, DLT type CBDCs should be ruled out since they have security loopholes which are not fixed yet.

References

- Adrian, Tobias and Mancini-Griffoli, Tommaso, 'The Rise of Digital Money' (July 2019) International Monetary Fund Fintech Note/19/1 <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>
- Bank for International Settlements: Committee on Markets and Payment Infrastructure, Market Committee, 'Central bank digital currencies' (March 2018) <https://www.bis.org/cpmi/publ/d174.pdf>
- Belke, Ansgar 'After the Bazooka a Bonanza from Heaven – „Helicopter Money" Now?' (2018) ROME Discussion Paper Series, No. 18-02
- Benes, Jaromir and Kumhof, Michael, 'The Chicago Plan Revisited IMF Working Paper Au-gust 2012' <https://www.imf.org/external/pubs/ft/wp/2012/wp12202.pdf > accessed 22 July 2019
- Benk, Szilárd; Kajdi, László; Kollarik, András; Mamira, Zoltán; Szebeny, Miklós; Török, Gergő and Varga, Lóránt, 'Digitalizáció és pénzrendszer' Fábián, Gergely and Virág, Barnabás (eds), *Bankok a történelemben: innovációk és válságok* (Magyar Nemzeti Bank 2018) 696
- Berentsen, Aleksander and Schar, Fabian, 'The Case for Central Bank Electronic Money and the Non-Case for Central Bank Cryptocurrencies' Review, Federal Reserve Bank of St. Louis (2018) 100 (2)
- Berman, Ana, 'IMF and World Bank Launch Quasi-Cryptocurrency in Exploration of Blockchain Tech' (*Cointelegraph*, 14 April 2019) <https://cointelegraph.com/news/imf-and-world-bank-launch-quasi-cryptocurrency-in-exploration-of-blockchain-tech?fbclid=IwAR2hrCpg42VOM7WI4jwFL5TSk57tWIDJog8NO5tB2g0S8Fc5uBOe8qL039k> accessed 1 August 2019
- Bujtár, Zsolt, 'A kriptovaluták európai és máltai szabályozásának összehasonlítása: A máltai sólyom szárnyalása' (2018) 18 (5) Európai Jog 6-16

- Carstens, Augustín, 'The future of money and payments: Speech by Mr Agustín Carstens, General Manager of the BIS, at the Central Bank of Ireland, 2019 Whitaker Lecture, Dublin, 22 March 2019' <https://www.bis.org/speeches/sp190322.htm> accessed 21 July 2019
- Cascarilla, Charles, 'Paxos standard white paper' (2018) <https://www.paxos.com/wp-content/uploads/2019/02/PAX_Whitepaper.pdf> accessed 22 July 2019
- De, Nikhilesh, 'Tether Lawyer Admits Stablecoin Now 74% Backed by Cash and Equivalents' <https://www.coindesk.com/tether-lawyer-confirms-stablecoin-74-percent-backed-by-cash-and-equivalents> accessed 12 June 2019
- Kecskés, András and Bujtár, Zsolt, 'Az árnyékbankrendszer jogi szabályozása az Egyesült Államokban és az Európai Unióban' (2017) 23 (1) JURA 266-277
- Kecskés, András and Bujtár, Zsolt, 'A kriptovaluta ökoszisztéma európai uniós és a svájci szabályozásának összehasonlítása' (2018) 24 (2) JURA 427-439
- Kumhof, Michael and Noone, Clare, 'Central Bank Digital Currencies - Design Principles and Balance Sheet Implications' (2018) Bank of England Working paper No. 725
- Simms, Thomas, 'China's Digital Currency Is Ready, Central Bank Says' (*Cointelegraph*, 11 August 2019) <https://cointelegraph.com/news/chinas-digital-currency-is-ready-central-bank-says> accessed 12 August 2019
- Szalay, Gábor, 'The Impact of the Lack of Transparency on Corporate Governance: A Practical Example' (2018) 1 (2) Corporate Law & Governance Review 21-28 <www.virtusinterpress.org/IMG/pdf/clgrv1i2p2.pdf> accesssed 12 July 2019
- Szalay, Gábor, 'A kriptovaluták nemzetközi szabályozási trendjei: Kriptotőzsdék és ICO-k értékpapírjogi perspektívából' (2019) 74 (3) Jogtudományi Közlöny 126-134

Short biography of the author

The author worked as a manager for 20 years in several commercial banks and securities firms in Hungary. He received his university doctorate degree in 1994 from the University of Pécs, Faculty of Economics and Business. His thesis focused on the comparative analysis of invest-ment funds regulation in the EU and Hungary. He started his PhD stud-ies in 2015 at the University of Pécs, Faculty of Law. His doctoral thesis focuses on the legal and economic aspects of securitization, while the main research areas include capital markets regulation, shadow bank-ing, corporate scandals from the perspective of corporate governance, and crypto asset regulation. Together with co-authors András Kecskés and Vendel Halász, the author published a comprehensive 1000 pages book titled Tőzsdeuniverzum, which focuses on the functioning of finan-cial systems with special attention to capital markets. The book is pub-lished by HVG-Orac publishing house.

Fluidity of term of cryptocurrency – a challenge for regulators

Sonja Bunčić* – Alpar Lošonc** – Andrea Ivanišević***

Abstract: Cryptocurrencies are innovative and controversial products of decentralized technology known as a blockchain with inherent encryption. They are intrinsically linked to the Internet; they are not subject to the control of institutions and are created by a group of people called miners who use software to solve mathematical problems. Vast expansion of this technology has brought cryptocurrencies to the attention of public authorities. However, legislative intervention in this area is only at its infancy.

The greatest challenge in the process of regulation of cryptocurrencies is to set a legal term for cryptocurrency. The main problem that has inspired this work is the fact that different countries of the world (US, Australia, Japan, EU, China) answer differently the same question relating to the definition of the cryptocurrency. So far, in the observed regulation, there have been two sides of legal definition. Some countries define cryptocurrency as money, that is, as a means of exchange, and there has even been an unsuccessful attempt to identify cryptocurrency as digital, electronic money. Other countries define cryptocurrencies as assets, trying to determine them as financial instruments, commodities, securities or property with the aim of preventing tax evasion.

Cryptocurrency has undoubtedly achieved the status of an exchange medium in a significant user community due to its ability to realize economic value, and there is basis for it to become a latent means of exchange. At the same time, cryptocurrencies have the potential to become immaterial assets and serve as a means of investing. The establishment of a unified definition would reduce uncertainty in their denationalized world and create a point that would allow regulators, in the future, to establish a balance between consumer protection and innovative freedom. Only then would this industry have the potential to embrace a wider customer base.

Keywords: cryptocurrencies, regulators, money, asset

1. Introduction

The paper was created as part of the project "Improving Serbia's competitiveness in the process of joining the European Union", No. 47028, funded by the RS Ministry of Education and Science.

* Professor, University of Novi Sad, Faculty of Technical Sciences.
** Professor, University of Novi Sad, Faculty of Technical Sciences.
*** Associate professor, University of Novi Sad, Faculty of Technical Sciences.

The occurrence of cryptocurrencies is, in a historical context, determined by two phenomena. The first is a crisis that broke out in 2007 and had significant financial aspects. The second one is the dynamics of digital technologies and their applications in relation to financial transfers. As for the first one, the cryptocurrency supporters hoped that they would overcome the possible monetary regressions (inflation / deflation, speculative bubbles, etc.). The supporters of the second phenomenon recognized the possibility of technology to replace standard financial mediation-based mechanisms by banks and state (a phenomenon called "disintermediation"[1] which entails deconstruction of the institutionalization of monetary sovereignty), or we can also say that cryptocurrencies were intended as means of dismissing something called in law a "disinterested third party", and that financial transfers are done in terms of "peer-to-peer payment network". We can at least briefly state that the ambitions of those who have promoted cryptocurrencies are not modest: the avoidance of an always non-neutral state with its monetary policy is offered as a technologically mediated realization of spontaneous "anarchist" intersubjective relations. This should be enabled by rules that rely on technological algorithms, and therefore on technological automatism that regulates arbitrariness (self-executing programs in the sense of "smart contracts")[2]. Given the fact that money is never just an instrument in human relations, cryptocurrencies project a profound transformation of exactly the same relationship. Instead of habitualizing trust without which standard money would be impossible, here the "fundamental trust embedded in money has simply been transposed into a 'machine code' "[3] in the sense of accounting automatization ("network ledger")[4].

The biggest legal challenge in regulating cryptocurrency is defining the term cryptocurrency (most often Bitcoin, as perhaps its most significant

[1] P. Vigna and M. Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (The Bodley Head 2015)

[2] L. Luu, DH Chu, H. Olickel, P. Saxena and A. Hobor, 'Making smart contracts smarter' in *Proceedings of the 2016 ACM-SIGSAC Conference* (ACM 2016) 254–269.

[3] Adam Hayes, 'The Socio-Technological Lives of Bitcoin Theory' (2019) Culture & Society 1–24.

[4] Nicholas Plassaras, 'Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF' (2016) 14 (1) Chicago Journal of International Law 377–407.

representative), or determining its legal nature.[5] Today, there is still no clear legal definition of this innovative phenomenon. The question is to what extent an extremely volatile phenomenon that undergoes constant transformations can be regulated at all, and to what extent the right can race with the dynamics of cryptocurrency: there is even Bitcoin 2.0. (just like b-money or bit gold, etc.), and at the time of writing this, the project Libra by agile Facebook has already emerged.

A key problem that has inspired this research is the fact that different countries of the world define cryptocurrencies differently. Definition of the notion and, therefore, the legal nature of cryptocurrency could reduce uncertainty; thus, it is a clear, predictable and comprehensive way to start a debate on how to regulate this new phenomenon related to the development of the internet and technology.

Analysis of the existing regulations and theoretical considerations of the issue relating to the definition of the cryptocurrency term have revealed two perceptions of the concept and legal nature of cryptocurrencies, especially the bitcoin. One perception tries to link cryptocurrencies with money, and the other tries to designate cryptocurrencies as a good, that is, "virtual" asset (good).Our attempt, in this paper, is to analyze both aspects which tend to define the term of cryptocurrency in different ways, thus enabling the development of regulations that would somehow regulate this area.

2. Perceiving cryptocurrencies as money

The first concept that relates cryptocurrencies, i.e. bitcoin, to the concept of money faces at least two problems. First, even when cryptocurrencies are accepted as money, legislations define them differently. Second, there is no single, completely satisfactory theory in economic or legal theory about what money is, which requires an analysis of the notion of money and its characteristics or functions, and a comparison with the functions that cryptocurrencies have as innovative "money".

The fact that the legislation defines cryptocurrency in different ways even when it is regarded as money confirms the analysis of valid

[5] M. Lambooij, 'Retails Directly Accepting Bitcoins: Tricky Tax Issues' (2014) (3) Journal of Derivatives and Financial Instruments 138-144.

regulation. Thus cryptocurrency is defined as: digital currency (Argentina, Thailand and Australia), crypto-token (Germany), payment token (Switzerland), cyber currency (Italy and Lebanon), electronic currency (Canada, Colombia and Lebanon).[6]

Generally speaking, when considering the concept of money as a legal category, there is a distinction in the literature between the views of those who represent the so-called *state theory* of money and those who support the *social theory* of money. The representatives of the state theory of money put the role of the state at the forefront which, as the bearer of monetary sovereignty, enjoys a legal monopoly in issuing money. In contrast to the state theory, the representatives of social theory believe that public opinion is crucial in determining the concept of money.[7] A general view of the theoretical conception of money indicates a completely different approach to its determination. Hence, the attempts to define cryptocurrencies as money and describe their characteristics with the characteristics of real, actual money give different results.

In order to overcome the problem of different perceptions of money, it is much easier to rely on the generally accepted notion that certain conditions must be fulfilled in order for certain currencies to be considered money. There are different economic and legal conditions that a particular currency must satisfy in order to be considered money. Classical economic theories define money by its functions. Money in the classical sense of the word must be: 1. Medium of exchange, 2. Unit of measurement, and 3. Serve to preserve the value.

The question is whether cryptocurrencies, i.e. bitcion as its representative, can be defined as money, or more precisely, whether it possesses some of the characteristics of money. Therefore, we will analyze all three characteristics of money accepted in classical theory and compare them with the characteristics of cryptocurrencies.

2.1. Money as a medium of exchange

[6] The Law Library of Congress, Global Legal Research Center, 'Regulation of Cryptocurrency Around the World' (2018) < https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf>

[7] M. Dimitrijević, 'Electronic money in modern monetary law' (2018) Collection of papers of Faculty of Law, Niš 2018/81 223.

Cryptocurrencies are decentralized and unlike real (*fiat*) money, they are not eligible to be considered money. In contrast to money, there is no central government (central bank) that controls the issuance of cryptocurrencies nor does it determine their intrinsic value. In order to make a comparative review and determine whether cryptocurrencies may or may not be regulated as money, we will consider some solutions from different laws.

We should start with the European Union, where cryptocurrencies are not accepted as money.[8]

The European Banking Authority, the European Securities and Markets Authority (European Insurance and Occupational Pensions Authority) have issued a warning[9] to consumers that cryptocurrencies are risky and linked to the possibility of cybercrime, as specific cryptocurrency law has not yet been enacted. This warning depicts the attitude of these financial organizations that they do not consider cryptocurrencies to be money, but it also indicates that this innovative phenomenon has not been fully understood by the official authorities. Regardless of this misconception, it is commendable that these financial institutions still accept the existence of cryptocurrencies and the need to protect the users against possible risks.

Therefore, all three organizations have tried to define the legal nature of cryptocurrency. The European Parliament's Report on Cryptocurrency [10] states that it is a "currently existing and accessible cryptographic digital presentation of value that is not controlled or guaranteed by the central bank or a public authority and that it does not have legal currency or money."

The view that cryptocurrencies cannot be considered money was also accepted by Australia. Cryptocurrencies are regulated by tax regulations according to which tax authorities do not accept this innovative

[8] European Central Bank defines a VC as a "type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" (*European Central Bank*, 2012) 14.

[9] <https://eba.europa.eu/-/esas-warn-consumers-of-risks-in-buying-virtual-currencies> related warning by ESMA <https://www.esma.europa.eu/press-news/esma-news/esas-warnconsumers-risks-in-buying-virtual-currencies> accessed 11 February 2018.

[10] Marek Dabrowski and Lukasz Janikowski, 'Virtual currencies and central bank monetary policy: challenges ahead' (July 2018).

phenomenon as money because ATO[11] does not see cryptocurrencies as either money or foreign currency.[12]

China's central bank, the National Bank of China (PBOC), has been conducting digital currency research for three years now and it has founded the Digital Money Institute within its National Bank (PBOC.) Zhou Ksiaochuan, the PBOC governor at that time, was working on the regulatory status of virtual currencies when, at a press conference held during the annual session of the National Congress of Nations in March 2018 he stepped down. According to Zhou, Chinese regulators do not recognize virtual currencies like bitcoin as a means of payment in retail such as paper money, coins or credit cards. The banking system does not accept any existing virtual currency nor will it provide any corresponding services, he said.[13]

The United States generally do not accept cryptocurrencies as money. The US Treasury Department's Financial Crimes Enforcement Network (FinCEN) does not recognize cryptocurrency as a "real currency" (legal tender), but recognizes administrators and account exchangers that have been converted to government currencies as "cash service companies" (MSBs), which means that they are subject to FinCEN registration, reporting and recordkeeping rules for MSBs (FinCEN, 2013)[14]. Later on, we will see that there are different definitions of cryptocurrencies within the United States, depending on the state, and that there is no uniform opinion on the definition of cryptocurrencies.

In contrast to the above regulations, Japan has accepted cryptocurrencies as a legitimate means of payment. Namely, the Law on Payment Services of April 2017[15] legalized the existence of cryptocurrency exchange offices. The amended Law on Payment

[11] Australian Tax Office.

[12] Australian Tax Office, 'Tax Treatment of Crypto-Currencies in Australia – Specifically Bitcoin' (last updated 21 December 2017) <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia--specifically-bitcoin/> archived at <https://perma.cc/UFZ7-QSUG>.

[13] Xiaochuan Zhou, 'Future Regulation on Virtual Currency Will Be Dynamic, Imprudent Products Shall Be Stopped for Now' (*Xinhuanet*, 1 March 2018) <http://www.xinhuanet.com/finance/2018-03/10/c_129826604.htm> (in Chinese), archived at <https://perma.cc/2CW7-8F2T>.

[14] FinCEN, 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (2013).

[15] Payment Services Act No. 59 of 2009, as amended by Act No. 62 of 2016.

Operations provided a definition of cryptocurrency[16]. This implies that cryptocurrencies in Japan are given one of the characteristics of money, such as a legitimate means of payment without the status of money in the classical concept, and it is determined as the value of the property.

Despite the fact that regulations and law do not see cryptocurrencies as money, they still have acquired characteristics of an exchange medium in everyday life. We read daily news articles and see various other proofs that cryptocurrencies, particularly the bitcoin, are used as a means of exchange. Most software and hardware companies have developed applications where services and goods can be paid in cryptocurrencies, and these companies also provide services that allow investors to invest in this currency.[17]

According to David Yermack,[18] real evidence of cryptocurrencies being a medium of exchange can be obtained from data existing in the universal ledger of bitcoin transactions. Most of these transactions are between speculative investors but about 26,000 of bitcoin transactions involve the purchase and sale of food or merchandise. It should certainly be noted that in a world with around 7 billion consumers, bitcoin is used for exchange purposes in an insignificant percentage when compared to the total number of transactions. Even though the percentage of bitcoin used for exchange is small relative to participation in general exchange, its presence is obvious and it is gaining an upward trend.[19]

[16] Payment Services Act art. 2, para. 5 defines cryptocurrency as property value that can be used as means of payment, purchase, rental, or provision of services by all persons, which can be bought or sold to anyone and transferred by electronic data processing system; or - property value that can be exchanged with anyone for higher property value and can be transferred by electronic data processing system.

[17] The most widely cited ranking of the top bitcoin merchants appears to be "The Bitcoin Ladder," https://en.bitcoin.it/wiki/Bitcoin_Ladder, but it is badly out of date, as it ranks the defunct and notorious Mt. Gox and Silk Road as the top two worldwide merchants.

[18] David Yermack, 'Is Bitcoin a Real Currency? An Economic Appraisal' (2013) National Bureau of Economic Research Working Paper 19747 <http://www.nber.org/papers/w19747> 9-10.

[19] The co-founder of bitcoin payment processor BitPay estimated the number of worldwide businesses at 26,000 in a separate interview given contemporaneously. See <http://money.cnn.com/2014/03/17/smallbusiness/bitcoin-bitpay>. However, it is widely understood that most of these transactions involve transfers between speculative investors, and only a minority are used for purchases of goods and services. For instance, Fred Ersham, co-founder of Coinbase, the leading digital wallet service,

Cryptocurrencies, therefore, serve as a medium of exchange, since they allow individuals to pay directly for goods or services with no commission for the transactions desired. As we noted in the previous presentation, they are not legal tender, but due to the presence of this innovative technology and its implementation, it would be more accurate to define cryptocurrency as a means of exchange rather than a means of payment.

This is supported by the hypothesis from the beginning that cryptocurrencies are not money but have one of its characteristics: they serve as a medium of exchange. In the EU, cryptocurrencies are not designated as money but are recognized as a medium of exchange. The European Central Bank stated: "For the sake of reminder, the definition of virtual currencies according to AMLD5[20] is as follows: 'a digital representation of value not issued or guaranteed by a central bank or public authority is not necessarily linked to a legal currency and does not have legal status of a currency or money, but they are accepted by individuals or legal entities as a medium of exchange, and they can be transferred, stored and traded electronically'."[21]

2.2. Money as a unit of value measurement and cryptocurrencies

estimated in the interview in March 2014 that 80% of activity on his site was related to speculation, down from perhaps 95% a year earlier (Goldman Sachs, 2014). If we take this estimate as correct, then perhaps 15,000 bitcoin transactions per day involve the purchase of a product or service from a merchant. In a world with 7,000,000,000 consumers, most of whom make multiple economic transactions each day, bitcoin appears to have an extraordinarily negligible market presence. Ersham further states in his interview that 24,000 merchants are registered with Coinbase.

[20] In the Fifth Anti-Money Laundering Directive (AMLD5), "virtual currencies" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored and traded electronically.

[21] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2013] OJ L156/43.

Unlike the previously analyzed function of money as a medium of exchange, where there is possibility for cryptocurrencies to be accepted as a specific medium of exchange, linking cryptocurrencies to the characteristic of money as a unit of measurement shows a number of weaknesses. There are several reasons that indicate that this feature represents a major weakness of cryptocurrency. In order for a currency (digital or real) to have this characteristic, and to be considered a unit of measurement, it must be able to determine its value in an easy and simple way with respect to other world currencies. It is highly debatable whether cryptocurrency, or bitcoin, fulfills this requirement. Most authors (Perkins, Cviter, Yermack) find that bitcoin has been facing numerous problems in the course of becoming a unit of measurement.

The first problem stems from its extreme instability. Its value against other currencies changes on a daily basis, every minute. We can easily check this feature by analyzing the change in the bitcoin value compared to dollar over the course of a day.[22] Accepting the bitcoin as a unit of measurement would be extremely expensive and impractical because of its extreme volatility.

The second problem arises from the "technical" definition of bitcoin as it is expressed with a value having at least 4 decimals. This creates great confusion and confusion among traders, and accepting bitcoin as a unit of measurement under these conditions would be a high cost of calculating bitcoin in other currencies.[23]

Therefore, we can conclude that cryptocurrencies do not qualify for this feature of money, and this is another reason why they should not be defined as money.

2.3. Money as means of value preservation and cryptocurrencies

[22] Yermack (n 18) 14: "As a result, many websites havetaken to relying upon unwieldy price aggregations, such as the average bitcoin price over several exchanges over the past 24 hours, but these aggregates do not indicate to merchants and consumers the true cost of procuring or selling a bitcoin at the present time."

[23] ibid. For instance, a visit to one online food retailer yields offers of a jar of salsa for 0.01694 BTC, chocolate bars for 0.00529 BTC, and a tea variety pack for 0.05255 BTC.

When considering this characteristic of money and its comparison with cryptocurrencies, the main question that arises is: Are cryptocurrencies stable and reliable enough to measure other values, or can they represent a measure of value that could serve as a means of preservation of value?

In the course of our analysis of money and its characteristic of being a means of preservation of value, the first thing to note is that the value of real money and its stability are controlled, but this control and maintenance of stability is subject to political and other influences. Unlike real money, cryptocurrencies are not subject to these influences, thus, it could be easily concluded that cryptocurrencies, free from political and other known influences, could have the characteristic of preserving values. This obviously strongly affects the value of already existing cryptocurrencies.

In addition, as technology and its development affect the stability of cryptocurrencies, personal relationship of an individual and his/her prediction and trust in particular cryptocurrencies are extremely important for their value. Thus, cryptocurrencies are completely unstable and unpredictable for value preservation which is why they could not satisfy the necessary conditions to be considered as a means of value preservation.

This brief analysis leads to a conclusion that cryptocurrencies could not be considered money; however, they are used as a medium of exchange in reality. In doing so, they are eligible to share only one characteristic of money and that is to serve as a medium of exchange. Yet, they cannot be categorized and defined as money.

3. Electronic money and an attempt to identify it as cryptocurrency

Electronic money has enabled virtual online payments. This money is not physically present but allows for easy transfer to electronic accounts and can be used for various purposes. Hence the idea of defining cryptocurrencies as electronic money.

Electronic money and cryptocurrencies are related to the internet and new, technological access to money, which is a similarity between them, but they can still not be identified based on that. First of all, the purpose of cryptocurrencies is much broader than that of issuing electronic money. Electronic money is considered to be merely a digital substitute for traditional currency banknotes and coins. Therefore, the legal definition

given by the Japanese (Sıddık-Yurtçiçek)[24] is necessary to realize the difference between electronic money and cryptocurrency. According to the author: "Electronic money is a digitalized monetary obligation, and therefore the definition of electronic money in the modern monetary literature is the one where electronic money is viewed as a set of information transmitted by issuing an electromagnetic amount based on a contractual obligation with an electronic currency issuer in order to fulfill a monetary obligation defined by a specific contract. "

Therefore, there must be a legal basis for issuance and use of electronic money. This can be found in laws, particularly those on the central bank, and laws governing commercial banks. Furthermore, it implies that electronic money is just another form or new functional application of real money. It is therefore under the control of the central government and subject to all regulations as cash is. Also, possible risks that electronic money is exposed to, as well as its online use and technological innovations require additional regulations by the state in order to protect consumers and ensure their safety in electronic transactions. Cryptocurrencies are not subject to these rules and they cannot be referred to as electronic money.

Electronic Money Directive [25] was adopted at EU level, but it is evident that the aim was not to include and regulate cryptocurrencies as it does not consider them electronic money. Unlike electronic money, cryptocurrencies are independent of the official national currencies and of their control and valuation.

According to the ECB, which made clear distinction from the possibility of considering cryptocurrencies as electronic money, estimated in its special publication [26] that bitcoin could not meet all the necessary conditions in order to be considered electronic money. It gives the

[24] M. Sıddık-Yurtçiçek, 'The Legal Nature of Electronic Money and the Effects of the EU Regulations Concerning the Electronic Money Market' (2013) (4) Law & Justice Review 276-321.

[25] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance) [2009] OJ L 267/7.

[26] European Central Bank, 'Report on Virtual Currency Schemes' (October 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> 10.

definition of electronic money.[27] Furthermore, the ECB states that the inability to identify electronic money with cryptocurrencies lies primarily in the volatile value of cryptocurrencies. The value of cryptocurrencies changes, as it is usually based on its own supply and demand. Monetary authority has no influence on that which means that the control over cryptocurrency is left to its issuer, which is usually a non-profit organization. In case of electronic money transactions, data on transfers and users are recorded while transactions with cryptocurrencies have anonymity as one of their important characteristics.

3.1. Summary of views on cryptocurrency regarded as money

We could say that no country in the world has accepted or recognized cryptocurrency as money. They are not recognized, legitimate means of payment because each country has its own currency that has the status of a legal tender. This implies that cryptocurrency cannot be accepted as a foreign currency either. Nevertheless, cryptocurrencies are in reality used as a medium of exchange for various goods and services, so they could provisionally be considered as a medium of exchange. Conditionality stems from its instability and limitation so, for now, we can consider it a latent and sometimes speculative medium of exchange.

4. Cryptocurrency as an asset– attempts to define it

Another understanding of cryptocurrencies and their legal qualification tends to qualify these currencies as an asset.[28] This qualification arose from the government's need to protect itself against tax evasion and the practice of money laundering. Thus, determination of cryptocurrency as an asset originates in the acts issued by the competent tax authorities or special anti-money laundering bodies. We can also find cryptocurrencies qualified as asset in the general institutes of legal science and the concepts of property.

[27] Electronic money is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction, but acting as a prepaid bearer instrument.

[28] Joanna Perkins and Jennifer Enwezor, 'The legal aspect of virtual currencies' (2016) Butterworths Journal of International Banking and Financial Law 203.

Property rights are part of personal right that governs subjective rights, so the property is a set of subjective property rights. These are the rights with their own monetary expression or which relate to an asset that can be expressed in monetary terms. Recent case law has sought to enable the categorization of rights as property in cases where those rights have acquired economic value and have shown that they are subject to transfer or trade. The hypothesis, therefore, is that cryptocurrency units, which have undoubtedly shown that they have an economic value and great transfer potential compared to other market participants and are sufficiently developed to be freely tradable, can be categorized as a type of property or asset by common law. However, this viewpoint is not generally agreed on and the categorization of cryptocurrencies as assets (usually virtual) in regulations that accept it as a type of property is made depending on the number of users as well as the scope and purpose that cryptocurrencies are used for. Namely, if cryptocurrencies are used as a means of investment on a larger scale, this leads to a conclusion that they represent property, and if they are predominantly used for buying and selling then they are considered as money.

When it comes to accepting cryptocurrencies as a property, there are different interpretations and perceptions about them as assets. We will explain some of these interpretations in more detail, especially cryptocurrencies as a financial instrument, a commodity or property, and a security.

4.1. Cryptocurrency as a financial instrument

Commodity production and credit system dictate markets to continuously create different instruments by which they register, transfer and realize monetary obligations from commodity turnover, holding money, credit, risk transfer from one subject to another, investments and the like. Investment in these instruments creates financial assets and not real assets. It is based on the principle that when someone buys an investment or capital value, that is, when they make investments, they buy the rights to the expected return. The connection between real and financial assets is achieved through financial markets, which is why these instruments are called financial instruments.[29]

[29] Sonja Bunčić, *Banking and stock market right*, (Poslovni biro SB 2012) 334.

Cryptocurrencies are widely used as an investment asset[30] and hence the desire of some regulators to refer to them as a financial instruments. However, there are reasons for rejection of this view. The definition of the term financial instrument is a matter of interest for both economic and legal science. Economic theory defines financial instruments based on the character and function of various financial instruments as an expression of the mobilization of monetary liabilities and receivables, starting from their basic function of money, which they express, as well as the nature of the liabilities they represent. Legal determination of financial instruments focuses on the enumeration system [31] while other legislation provide the definition of the basic types of financial instruments in relation to their characteristics,[32] and individual legislation give a general definition of financial instruments [33].

The given definitions imply that a financial instrument can also a financial derivative such as currency, commodity, security and various other statistical indicators, indices and percentages. So, if cryptocurrencies cannot be regarded as commodity or securities, they cannot be categorized as financial derivatives nor will they be treated as financial instruments.[34]

For the time being, most states take the view that cryptocurrencies cannot be financial instruments, but are specific and yet undefined "virtual" assets. The idea of "virtuality" and identification of bitcoin as a virtual asset helps a bit in resolving the situation: there is a virtual dimension even with the standard form of money. Namely, we know that the present form of money is fiat-money and this does not rely on physical matter which destroys the classic maxim, *ex nihilo nihil fit*. Monetary theory has long been pointing out that money is created by banks, that is, financial intermediations, and that they are creative in the sense of

[30] However, it is widely understood that most of these transactions involve transfers between speculative investors, and only a minority are used for purchases of goods and services. For instance, Fred Ersham, co-founder of Coinbase, the leading digital wallet service, estimated in a March 2014 interview that 80% of activity on his site was related to speculation, down from perhaps 95% a year earlier (Goldman Sachs, 2014).

[31] USA Law on Securities from 1933 gives enumeration of financial instruments.

[32] In England, Financial Services Act from 1986 lists instruments and defines their characteristics.

[33] Slovenian Law specifies financial instruments as securities issued in a series.

[34] Irina Cvetkova, 'Cryptocurrencies Legal Regulation' (2018) V (2) BRICS Law Journal 135.

creating out of nothing. This is the phenomenon of "credit money".[35] Also, it is interesting that bitcoin proponents are constantly invoking the material determination of bitcoin, that is, they want to go beyond the purely virtual image of bitcoin using phrases such as "digital metallism", or "one key aspect of Bitcoin's appeal to its advocates and supporters qua money - and an important reason for its rising price up until recently - is that the currency effectively mimics the properties of gold in virtual form".[36] This means that bitcoin proponents want to exit the virtual and find a "non-virtual" medium.

4.2. Cryptocurrencies as commodity or property

Commodity can be defined as tangible or intangible object with some economic value. Some legislation, especially the Anglo-Saxon one, have tried to define cryptocurrencies as commodities or even property for their specific characteristics (the possibility of attaching economic value).

So, in 2014, ATO[37] came to decision that bitcoin could not be considered a foreign currency, which we discussed earlier in more detail, but a means of exchange (*barter*).[38] As bitcoin is neither money nor a foreign currency, the ATO has argued that transactions performed by cryptocurrencies are no different than exchange operations, just like the exchange of goods, so they should be treated as such, from a tax-legal aspect. This is an attempt to indirectly treat cryptocurrencies based on their purpose, which is the exchange of goods, and to put taxes on them accordingly. Different qualifications of cryptocurrencies as money, commodity, property or financial instruments indicate that each country aims at adopting its own regulations in order to establish control over the operations or results of operations with cryptocurrencies.[39]

In the US, depending on the country or institution, there are different opinions about how cryptocurrencies should be understood. The

[35] M. Aglietta and A. Orléan (eds.), *La monnaie souveraine* (Odile Jacob 1998)

[36] Nigel Dodd, 'The Social Life of Bitcoin' (2017) Theory, Culture & Society 1–22, 8.

[37] Australian Taxation Office.

[38] Modern antropology believes that barter is rather a myth than a real instrument from history,

[39] 'New IRS Notice Confirms Tax Treatment of Bitcoins as Property and not Currency - Expected To Increase Popularity for Self-Directed IRAs, According to IRA Financial Group' (*Cision PrWeb*, 25 March 2014) <http://www.prweb.com/releases/bitcoins-self-directed-/ira-taxproperty-currency/prweb11704323.htm> accessed 18 June 2018.

Commodities Futures Trading Commission thought that cryptocurrencies should be viewed as commodities. In 2014, the CFTC had its first attempt to categorize bitcoin and other types of cryptocurrency under the term commodity as defined under Commodity Exchange Act 7 U.S.C. 1-27.[40] On the other hand, for tax purposes, the Internal Revenue Service (IRS) categorized cryptocurrencies as property or capital asset. [41] This is, once again, the confirmation of our view that the regulator defines cryptocurrencies only in relation to the interest that individual control bodies might gain from the area (payment, investment, savings) in which the cryptocurrencies are most used.

At the heart of the many regulatory issues surrounding virtual currencies is the question of how to classify this new and allegedly devastating technology into traditional property and personal rights developed by law. Lord Wilberforce: "... Before any right or interest can be categorized as property or right affecting property, it must be defined, recognized by third parties, capable of being accepted by third parties and of a degree of permanence or stability". [42] Cryptocurrencies can hardly meet these conditions, especially to be recognized and accepted by third parties, to have some degree of stability or durability, and to be defined is the condition least possible to fulfill. Recognition of cryptocurrencies as a commodity or property depends on further development of technology when creation of "virtual asset" could be a new category of assets with specific characteristics.

4.3. Cryptocurrencies as securities

Whether cryptocurrencies are securities is a very controversial question. The general definition of a security is that it is a document obliging its issuer to fulfill the obligation recorded on that document by its rightful holder. It is necessary, therefore, that we have the security itself,

[40] See In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29 <http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf>

[41] At the heart of many of the regulatory questions which surround virtual currencies is the question of how to allocate this new and, allegedly, disruptive technology to the traditional categories of property and personal rights developed by the common law.

[42] Perkins and Enwezor (n 28) 570.

the license for its issuance, and that it obliges the issuer to fulfill the stated obligations therein.

The idea to address this issue arose from the emergence of "ICO" (Initial Coin Offering) that issues tokens. A token is a unit of value issued by a private organization in a blockchain system. Investigating the situation in the case of DAO blockchain, the Securities and Exchange Commission of the United States of America stated that ICO should be considered a securities issue, regardless of the consequences that the investor may have. [43]

On the other hand, there are a number of opponents [44] of this view who emphasize that this is not a matter of security issuance and that it is not an "IPO" or an initial public offering of stocks, but that they are specific projects. They contain no obligation in terms of rights or money. Projects offer some kind of exchange and have nothing in common with securities except the idea of financing themselves by offering investors their virtual currency in exchange for most typically - nothing.

In addition, the issuance of cryptocurrency is decentralized and does not meet the concept of issuing securities. Also, any payment system participant can be the issuer because the transaction creates a new block in the chain of transactions. Therefore, there is not a single element that could categorize cryptocurrencies as securities.

4.4. Summary of views on cryptocurrencies regarded as property

Recognizing the new reality of the digital world has led to acceptance of the extension of traditional legal understanding of property. Hence the desire to have a digital form of cryptocurrency values accepted as a possible specific property as they enable the cryptocurrency holders to electronically possess them and make mutual payments and exchange virtual values. It should be noted that the value of this specific asset is based on the belief of its holders that its virtual, digital form has a real value. Thus, in today's world, some tax authorities, in an effort to establish

[43] U.S. Securities and Exchange Commission, 'SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities: U.S. Securities Laws May Apply to Offers, Sales, and Trading of Interests in Virtual Organizations' (25 July 2017) <https://www.sec.gov/news/press-release/2017-131> 18 June 2019.

[44] Cvetkova (n 34) 136.

control over cryptocurrencies and include them in their tax portfolio, have accepted that there is an argument for accepting cryptocurrency as a new form of property.

According to previous observations on cryptocurrency definition, we can conclude that the dominant view is that cryptocurrency is a specific type of property in a digital form which its owners can hold or exchange electronically, and use it to make payments in accordance with the belief that this virtual form has a real value. This conclusion is predominantly based on the 2014 EBA Opinion on cryptocurrency.[45]

5. Concluding considerations

Analysis of different definitions of cryptocurrency should, at least to some extent, provide answers to the questions: Is cryptocurrency a replacement for a classic coin? Is it a specific property? What is its future or is it just a temporary "optimism trade"? [46]

Cryptocurrencies are decentralized and innovative system that functions as an individual system and develops without a supervisory central authority. At the same time, critics point to the hidden elements and consequences of cryptocurrencies; namely, the fact that they have, despite promises, brought new forms of centralization, as well as the forms of distribution that do not suit the libertarian-anarchist projections of the founders. The same critics point out that those who engaged in cryptocurrency trading and were offered to "isolate" themselves from the dominant capitalist relations failed in this (bitcoin as the realization of "anti-system-like" orientation, "counterpower", "horizontalism" instead of verticalism,[47] transformation of the relation between public and private spheres).

Since 2008, we have witnessed the emergence of the first cryptocurrency, the Bitcion, which had its ups and downs and was the matrix for the creation of many other cryptocurrencies. There was loud criticism and deep concern that this system would affect existing economic and monetary stability, and would be used for various criminal

[45] <https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies>

[46] M. Babić, 'Kriptovalute-računalna provokacija, monetarno-finansijskam oda ili budućnost' (2018) (1) Pravni život 430.

[47] Dodd (n 36).

activities (money laundering, terrorist financing, or tax evasion, etc.). Although the Bank of Canada suggested that small, independent payment systems should not be too controlled and regulated, as they are certainly not too big a threat to the Canadian financial system (George-Cosh, 2014), [48] one should be very careful. This is one of the reasons that countries with smaller and less attractive financial markets do not regulate cryptocurrencies but have adopted a "watch and wait" strategy. After all, the contradictory reactions of the central banks regarding the already mentioned Libra are also indicative. The case of Ross Ulbricht and Silk Raod also point to a danger [49] which proves the inherently existing criminal dimension of cryptocurrencies. Besides, the cryptocurrencies have not proven to be resistant to excessive speculations (at least not in 2011 and 2017).

A review of the existing regulations shows that the definition of cryptocurrencies is something that only countries with developed markets have dealt with. There is a disagreement on the definition of cryptocurrencies. We have presented different perceptions of cryptocurrency as money, digital money, a medium of exchange. Others, however, have accepted to define cryptocurrency as a good or even some kind of financial property only for tax purposes. Some of the above regulations are formal, while in some cases the regulations are made by simply accepting the operations with cryptocurrencies. [50] We believe that these differences in the definition of cryptocurrency arise because the states tend to control and regulate the operations involving cryptocurrencies that are dominant on their market. This means that if cryptocurrencies are used as an investment instrument, then they will be designated as a type of financial property, and if used for the purchase and sale of goods and services, then they are defined as money and the like.

Technological development and operations with cryptocurrencies will continue to evolve, and those countries that have so far ignored or even banned them will not be able to remain indifferent and isolated from the spread of this global phenomenon. The future development of

[48] D. George-Cosh, 'Canada says bitcoin isn´t legal tender' (16 January 2014) <https://blogs.wsj.com/canadarealtime/2014/01/16/canada-says-bitcoin-isnt-legal tender/?KEYWORDS=bitcoin>.

[49] <https://sr.wikipedia.org/srec/Put>

[50] Alexander Radivojević, 'Virtual currencies and regulations' (2018) (29) Economic Ideas and practice 69.

cryptocurrencies will require their moving from the unregulated to the regulatory framework. Their designation as money or good will depend on technological development and the predominant purpose for which they will be used. It is important not to neglect the cryptocurrency phenomenon in relation to the analysis of the market. The purpose of creation of cryptocurrencies was a decentralized, liberal system versus controlled capitalism. A Citigroup analysis of bitcoin from 2017 found that "47 individuals held about 30%, another 900 held further 20%, the next 10,000 about 25% and another million about 20%." No country on earth has such an unequal distribution of assets and wealth. Is this how the mask of a liberal, decentralized cryptocurrency project falls?

The adoption of a single cryptocurrency concept is not yet realistic to expect today, primarily because of little knowledge about this innovative system and the difficulty in accepting and acknowledging its global strength and capabilities. Regulators should not only serve as a virtual currency exchange service in the denationalized world of cryptocurrencies, but they should also take on the role of a supervisor as agents of miners verifying electronic transactions, thereby enhancing consumers' security and confidence. Only then could they be sure that this whole system of cryptocurrencies will not become just "trading with optimism"[51].

References

- Babić, M., 'Kriptovalute-računalna provokacija, monetarno-finansijskam oda ili budućnost' (2018) (1) Pravni život 430
- Aglietta, M. and Orléan, A. (eds.), *La monnaie souveraine* (Odile Jacob 1998)
- Australian Tax Office, 'Tax Treatment of Crypto-Currencies in Australia – Specifically Bitcoin' (last updated 21 December 2017) <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/> archived at <https://perma.cc/UFZ7-QSUG>

[51] Babić (n 46) 431.

- Bunčić, Sonja, *Banking and stock market right*, (Poslovni biro SB 2012) 334
- Cision PrWeb, 'New IRS Notice Confirms Tax Treatment of Bitcoins as Property and not Currency - Expected To Increase Popularity for Self-Directed IRAs, According to IRA Financial Group' (25 March 2014) <http://www.prweb.com/releases/bitcoins-self-directed-/ira-taxproperty-currency/prweb11704323.htm> accessed 18 June 2018
- Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29 <http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf>
- Cvetkova, Irina, 'Cryptocurrencies Legal Regulation' (2018) V (2) BRICS Law Journal 135
- Dabrowski, Darek and Janikowski, Lukasz, 'Virtual currencies and central bank monetary policy: challenges ahead' (July 2018)
- Dimitrijević, M., 'Electronic money in modern monetary law' (2018) Collection of papers of Faculty of Law, Niš 2018/81 223
- Dodd, Nigel, 'The Social Life of Bitcoin' (2017) Theory, Culture & Society 1–22
- European Banking Authority, <https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies>
- European Banking Authority, 'ESAs warn consumers of risks in buying virtual currencies' (12 February 2018) <https://eba.europa.eu/-/esas-warn-consumers-of-risks-in-buying-virtual-currencies>
- European Central Bank, 'Report on Virtual Currency Schemes' (October 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
- European Securities and Markets Authority, <https://www.esma.europa.eu/press-news/esma-news/esas-warnconsumers-risks-in-buying-virtual-currencies> accessed 11 February 2018
- FinCEN, 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (2013)

- George-Cosh, D., 'Canada says bitcoin isn´t legal tender' (16 January 2014) <https://blogs.wsj.com/canadarealtime/2014/01/16/canada-says-bitcoin-isnt-legal tender/?KEYWORDS=bitcoin>
- Hayes, Adam, 'The Socio-Technological Lives of Bitcoin Theory' (2019) Culture & Society 1–24
- Kavilanz, Parija,'My business accepts Bitcoins' (*CNN Business*, 17 March (2014) <http://money.cnn.com/2014/03/17/smallbusiness/bitcoin-bitpay>
- Lambooij, M., 'Retails Directly Accepting Bitcoins: Tricky Tax Issues' (2014) (3) Journal of Derivatives and Financial Instruments 138-144.
- Luu, L.; Chu, DH; Olickel, H.; Saxena, P. and Hobor, A. 'Making smart contracts smarter' in *Proceedings of the 2016 ACM-SIGSAC Conference* (ACM 2016) 254–269
- Perkins, Joanna and Enwezor, Jennifer, 'The legal aspect of virtual currencies' (2016) Butterworths Journal of International Banking and Financial Law 203
- Plassaras, Nicholas, 'Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF' (2016) 14 (1) Chicago Journal of International Law 377–407
- Radivojević, Alexander, 'Virtual currencies and regulations' (2018) (29) Economic Ideas and practice 69
- Sıddık-Yurtçiçek, M., 'The Legal Nature of Electronic Money and the Effects of the EU Regulations Concerning the Electronic Money Market' (2013) (4) Law & Justice Review 276-321
- The Law Library of Congress, Global Legal Research Center, 'Regulation of Cryptocurrency Around the World' (2018) < https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf>
- U.S. Securities and Exchange Commission, 'SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities: U.S. Securities Laws May Apply to Offers, Sales, and Trading of Interests in Virtual Organizations' (25 July 2017) <https://www.sec.gov/news/press-release/2017-131> 18 June 2019

- Vigna, P. and Casey, M., *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (The Bodley Head 2015)
- Yermack, David, 'Is Bitcoin a Real Currency? An Economic Appraisal' (2013) National Bureau of Economic Research Working Paper 19747 <http://www.nber.org/papers/w19747>

Zhou, Xiaochuan, 'Future Regulation on Virtual Currency Will Be Dynamic, Imprudent Products Shall Be Stopped for Now' (*Xinhuanet*, 1 March 2018) <http://www.xinhuanet.com/finance/2018-03/10/c_129826604.htm> (in Chinese), archived at <https://perma.cc/2CW7-8F2T>

Virtual Currencies – Legal Challenges

Zsolt Halász*

Abstract: The appearance of the virtual currencies raises several legal questions beside their economic nature and features. What can they be used for? Can they fulfil a real payment function like the traditional currencies? The very general question is whether virtual currencies (their issuance and/or usage) need to be regulated and if yes, how to regulate? Beside the general questions, there are also several particular issues, like among others payment of taxes, salaries, lending and borrowing in virtual currencies, the application of anti-money laundering regulations, and last but not least the difficulties caused in law-enforcement. This paper tries to collect those questions which are to be answered by legislators in the not too far future.

Keywords: virtual currency, monetary system, risks, sovereignty

1. Introductory remarks

In the last couple of years, no single day could slip away without several news on the market and technology of the virtual currencies. It seems there is significant public interest towards the virtual currencies (VCs) comparable with the traditional or fiat currencies.

Beside the remarkable enthusiasm, there are still several essential open questions to be raised and answered on the nature and operation of the VCs, which were fundamentally necessary for their everyday usage. There are several generic issues related to VCs like:

- Why should the VCs be regarded as real money?
- What factors influence their value?
- Do VCs need to be regulated?
- Can VCs be regulated?
- If yes, what elements and how to be regulated?
- Are VCs means of payments or are they financial instruments for investment services?
- Can VCs be real alternatives of the traditional currencies?

* Associate professor, Péter Pázmány Catholic University, Faculty of Law, Financial Law Department (Budapest), halasz.zsolt@jak.ppke.hu.

- Can VCs take the place of the traditional currencies sometime in the future?

Beside the general questions one can endeavour specific related topics like the usage of VCs in taxation, lending, savings, payment of salaries etc.

Obviously both lists can be further extended. Hence before digging into the details, it is necessary to make clear some essentials.

Firstly, one has to make clear that the VCs' concept and their issuance is definitely different from electronic money, even if both operate in electronic environment and on basis of digital technology. VCs are different and independent from fiat currencies. Electronic money is issued against traditional money. VCs can be purchased or mined. The value and accounting of the VCs are independent from that currency from which the exchange has been happened.

Currently, VCs are legally not regulated, they are digital moneys based on the internet, mainly but not exclusively on the blockchain and the distributed ledger technology. Issuers or creators of the VCs are not central banks entitled to issue banknotes and coins on behalf on the state. Creators are developer groups without any central authority. Users of the VCs are members of internet's growing virtual community.

According to the definition used by the European Banking Authority VCs are a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment, and can be transferred, stored or traded electronically. The main actors are users, exchanges, trade platforms, inventors, and e-wallet providers[1]. European Central Bank uses a very similar definition in its report on virtual currencies. ECB highlights that key actors of the VCs are neither regulated nor supervised and users do not benefit from legal protection such as redeem ability or a deposit guaranty scheme, and are more exposed to the various risks that regulation usually mitigates.[2]

Nowadays, there are more than 2450 VCs are existing, however this number can change at any time, due to the unregulated and uncontrolled creation and issuance of them. Practically, anyone can create his/her own

[1] European Banking Authority, 'EBA Opinion on 'virtual currencies'' (4 July 2014) EBA/Op/2014/08.

[2] European Central Bank, 'Virtual Currency Schemes – further analysis' (February 2015)

VC. In August 2019, the market capitalization of the VCs was around USD 278 bn equivalent to HUF 80 trillion or Hungary's 2 years' GDP. Bitcoin's share of the whole market is around 68%[3]. The number and market of the VCs are constantly growing. Since beginning of 2018 the number of the VCs has grown by 1000. In 2017 the number of VC users were estimated between 2.9 and 5.8 million users[4]. In 2019 one can observe 300.000 to 450.000 VC transactions daily[5].

The novelty and even appearance of virtual currencies – in most cases, but not exclusively – is based on the development and existence of the blockchain technology. This technology, unlike a traditional centralized monetary system, operates in a decentralized IT system, in other words in a shared database. Without analysing its details, I would only emphasize here one main characteristic of this system, namely compared it to the computational operations performed on the traditional IT systems where the operations can be subsequently modified, it is not possible in the blockchain, where the system is unbreakable (until no one have 50%+1 of computers attached to the system). This feature undoubtedly promotes the use of technology in payment transactions. The possibility of creating a non-manipulatable and – within the system – cheaper payment system[6] through the virtual currencies is undoubtedly an important positive factor.

For the usage of VCs as means of payment it is necessary to have a limited number available of them. (However, if we consider that the number of virtual currencies cannot be restricted, anyone can create a new one, this allegation is less likely to be in place). Further advantage is the faster transaction implementation compared to traditional payment systems, transaction costs are cheaper and the system is more secure than a traditional payment system due to its non-centralized nature.

A question emerges, however, whether VCs can be real alternatives to the traditional ones issued by the central banks? A further question is how to classify them: as means of payment or investment, or both, or none of them? And furthermore, whether it is necessary to regulate their operation and usage?

[3] See data on <coinmarketcap.com>.

[4] Garrick Hileman and Michael Rauchs, 'Global Cryptocurrency Benchmark Study 2017' (University of Cambridge) 10.

[5] Source of the figures: <www.blockchain.com>.

[6] The cheapness is to be understand within the system only, because commission fees are usually added to the exchange operations between traditional and virtual currencies and there are certain differences between bid and sell rates either.

Any payment system can operate only in case of the users – a whole society – *trust* in the proper operation of the monetary system – namely in the state and the central bank (in its monetary policy, flexibility and ability to make proper decision when needed) and also in the commercial banks (backed by the prudential regulations, the central banks, the supervisory authorities and the deposit guarantee schemes) – since this is one of the core elements of the economy, the trade, the everyday life. The appearance of the VCs relates to the question of this trust in the traditional monetary system, or the attenuation of it – especially at the time and after the last financial crisis. The trust has weakened in the traditional monetary system and became stronger in unknown developers and officially uncertified IT systems....

2. Can VCs become real money of everyday usage?

To approach this question from theoretical side, it worth to analyse whether VCs will ever be able to reach a level of development when they can work as real money by looking at the concept and functions of money itself. András Vígvári pointed out that the emergence of money was closely linked to the increasing degree of division of labour and specialization: money emerged when the exchange of labour activities and products was replaced by the exchange of activities' outcomes[7].

Money first appeared in the form of commodity money. The ancient Greeks distinguished three main functions of money: means of counting, means of exchange, and reserve asset.

Jean Bodin, who was the first to describe the concept of sovereignty, regarded the issuance of money as one of the main or substantial attributes of sovereignty. „There is nothing of more moment to a country, after the law, than the denomination, the value, and the weight of the coinage"[8]. In other words, according to Bodin, the definition and issuance of the money – as a part of sovereignty – is an exclusive and non-transferrable right of the state, the sovereign.

Karl Marx identified five different functions of money[9]:

- measure of values (expresses the value of commodities),

[7] András Vígvári, *Pénzügy(rendszer)tan* (Akadémiai Kiadó 2008) 74.

[8] Jean Bodin, *Six books on the Commonwealth*, Chapter X: The true attributes of sovereinty.

[9] Karl Marx, *Das Kapital*: *Kritik der politischen Öekonomie* (first edition, Verlag von Otto Meissner 1867).

- means of circulation (provides the exchange of commodities),
- means of payment,
- formation of value/reserves,
- universal money.

Max Weber classified money as means of circulation and means of exchange. Money becomes means of payment through state regulation. According to Weber, money is emerged by state will and state regulation. The modern state keeps in its own hands the monopoly of monetary system regulation and money issuance. Money is kept alive by legal state force. The main function of money is to settle various debts (paying taxes to the state, paying interest payments by the state, etc.). The state collects taxes to finance its own needs and public functions, and the simplest form of tax collection in a general means of exchange instead of various forms of commodities. Since the usage of money as universal means of exchange is provided by legal state force, its main function will be the payment function [10].

The European Central Bank analyses the operation of VCs on the basis of the following main functions of money:

- medium of exchange,
- store of value, and
- unit of account[11].

The fundamental question for the regulation of money and the monetary system is: who creates the money and where does it stem from? Is it created by the state through regulation as Weber says or as Prof. Tibor Nagy points out „money is not created by state regulation, because it's emerged spontaneously."[12] István Simon adds that entities - not necessarily the national states exclusively - having sufficient power try to extend their power to money issuance because it brings economic benefits on the one hand, and on the other its political yield is also significant, namely by control over the economy.[13]

The European Court of Justice also had to analyse the nature and operation of the VCS. The Court had to answer the question in a preliminary ruling procedure: whether transactions, which consist of the

[10] Cf. in details Max Weber, *Wirtschaft und Gesellschaft* (Mohr 1922).
[11] European Central Bank (n 2) 23.
[12] Tibor Nagy, 'A pénzrendszer joga' in István Simon (ed) *Pénzügyi Jog I*. (Osiris 2007) 275.
[13] István Simon, 'Állandóság és változás a pénz jogi szabályozásában' in: István Simon (ed) *Tanulmányok Nagy Tibor tiszteletére* (Szent István Társulat 2009) 253.

exchange of traditional currency for units of the 'bitcoin' virtual currency and vice versa, in return for payment of a sum equal to the difference between, on the one hand, the price paid by the operator to purchase the currency and, on the other hand, the price at which he sells that currency to his clients, constitutes the supply of services for consideration within the meaning of the relevant article of the VAT Directive? In its ruling the Court declared „bitcoin virtual currency, being a contractual means of payment, cannot be regarded as a current account or a deposit account, a payment or a transfer. Moreover, (...) the 'bitcoin' virtual currency is a direct means of payment between the operators that accept it. Transactions involving non-traditional currencies, that is to say, currencies other than those that are legal tender in one or more countries, in so far as those currencies have been accepted by the parties to a transaction as an alternative to legal tender and have no purpose other than to be a means of payment, are financial transactions. It is common ground that the 'bitcoin' virtual currency is neither a security conferring a property right nor a security of a comparable nature.[14]

It should be noted that the European Central Bank represent an opposite view on VCs. According to the ECB VCs are not used widely to exchange value, they are not legally money, and – in the absence of minted versions – they are not currency either, and no virtual currency is a currency. However, it doesn't exclude to use VCs as contractual moneys between private parties.[15]

Four centuries after JEAN Bodin a completely new theory on the money (currency) and on its relationship to the state has been published by Nobel laureate Friedrich-August Hayek[16], who has described the concept of the private – non-state-issued – money. Hayek's concept preceded by three decades the factual appearance of the first VCs. According to Hayek's concept, the state's right for money issuance would be abandoned, and the monetary policy as we know it would not exist.

3. Legal issues and dilemmas

[14] Judgment of 22 October 2015, *Hedqvist*, C-264/14, EU:C:2015:718.
[15] European Central Bank (n 2) 24.
[16] Friedrich August Hayek, *Denationalisation of Money* (Institute of Economic Affairs 1976).

There are a number of legal dilemmas about the functioning and especially the usage of VCs. Here, one should not simply refer to the current regulations declaring a currency as official currency in a country[17] and to the fact that each traditional currency is declared to be an official currency in at least one country.

My legal dilemmas are more focused on the legal consequences and risks associated with unregulated nature of this issue and furthermore whether it is possible and/or necessary to create any kind of regulation.

Our traditional financial system operates on the fundament of a number of important factors, however this system has gone through a number of important changes, including the legal basis, in the not too distant past. Let us just refer here e.g. to the Bretton Woods rules and the elimination of the gold standard.

Among the referred factors two elements are to be highlighted as a basis of the current monetary system:

- the legal background: official currencies are to be accepted as official means of payments, and
- the trust in the financial intermediary system.

Official currencies are not exclusive means of payment, however certain payments (e.g. that of taxes) generally have to be implemented in official currencies. While legal regulation is difficult to be disrupted, a financial crisis can easily originate distrust in the traditional monetary and banking system. After the 2008 crisis the trust has partially eliminated, which might have initiated the creation of the first VCs. However, as we have seen, the idea of private money was not new.

In addition, other aspects may arise, such as the novelty nature or the promise of fast, safe and cheap payments. This promise is based on a new kind of technological operation that allows financial transactions to be implemented directly between virtual wallets bypassed the traditional banking system. In most cases, transactions are implemented in the blocks of the blockchain, which guarantees the secure implementation of the transaction in two ways. On the one hand, the blocks contain the data of all previous transactions (e.g. the elements of the ownership chain)

[17] Cf. According to Art. K) of the Basic Law of Hungary the official currency of Hungary shall be the Hungarian Forint. Further reading: Zsolt Halász, 'Public Finances' in András Zs. Varga, András Patyi and Balázs Schanda, *The Basic (Fundamnetal) Law of Hungary – A Commentary of the new Hungarian Constitution* (Clarus Press 2015) 321-343.

except for the identity of the participants in the transaction and on the other hand the authentication is done by the user community.

In principle the system is able to implement transactions quickly, although this advantage is less and less significant due to the development of traditional payment systems.

However, it is important to see that we must face risks beside positive features. First and foremost, we need to emphasize the complete non-regulated nature of the VCs and their operation, technology are not officially certified either. Virtual currencies are not created by any central bank, nor by a financial institution. They are created by private actors. As a result, the basis of the operations is the – blind – trust in the unknown creator/issuer, and/or the technology created by it, without any kind of legal guarantee. Until now, it is not possible to know exactly who created the most popular virtual currency, the Bitcoin. There is neither a contractual link, nor any legal protection if any unexpected loss or damage occurs related to the transactions with VCs. In fact, such losses happen. The state regulation of a monetary system has lent and generally lends - stronger or weaker, and sometimes varying - confidence in the legal tender in the course of history.

The system and technology promise anonymity to the users equivalent to cash. The virtual currency system allows anonymous ownership and anonymous transfers between users with a virtual wallet. The identification requirements and practice are less strict than in the traditional financial services. I do not think there is a need for a detailed explanation of how such a loose system can be used for tax evasion, money laundering and other illicit purposes. Furthermore, the anonymity is just pseudo-anonymity in case if many VCs (e.g.: Bitcoin) and the users can be tracked back. In case of other VCs (e.g.: Monero, Z-cash) the anonymity is real, raising real concerns related to the above-mentioned activities.

A substantial feature of this system and technology is the global access and usage, even if the freedom of usage and mining of VCs is divergent around the world. (In Europe or in the US they are not banned or restricted, but in certain countries like China or India.) This can also be a major advantage in many places that will allow a reduction in the number of conversion transactions between different currencies, however it also poses serious threats to the easy movement of money stemming from crimes or other illicit activities.

In the case of traditional currencies, it is important to recognize the ability like the issuing central bank to create money and to adjust the volume of money in circulation to the needs of the economy. For virtual currencies, we need to make two comments. On the one hand, due to the mathematical logic of the system, in case of several VCs the possible quantity is limited from the top and this quantity can be predetermined. For Bitcoins, this is 21 million units, which can be divided into 8 decimal places. Thus, the issuable quantity of virtual money is foreseeable and can be easily determined however this quantity is not flexible and thus less able to meet the varying needs of the economy. It is also important to point out that since no one and nothing limits the creation of new virtual money, there is no obstacle to the creation of additional VCs beside the currently popular ones. Right now, we know more than 2450 VCs and no one can predict the potential further increase of their number.

Last but not least, it is important to mention that the costs of transactions of the VCs are considered to be low, although conversions to and from the traditional currencies can bear significant transaction fees in addition to the difference between buying and selling rates. At this level of costs, the extreme volatility of the exchange rate is also a question that developers and users have to face. Many see this as a kind of investment opportunity, which, however, involves extreme risks due to the nature of virtual currencies.

It is therefore necessary to ask the fundamental question: how to classify and define the VCs and consequently how can/should they be regulated.

According to our recent knowledge, it's hard to answer these questions. It is not easy to answer what was the purpose of creating more than 2450 different virtual currencies. We cannot exactly see the different purposes of their creators. We do not know which ones will really exist in the future and until when and for what reason (uninteresting for the user, or upon creators will) will any of them cease to exist, and how will the exit from the market happen.

We know that instead of the traditional monetary system, there are ideas to create a safe monetary system free from external influences. We have seen that blockchain technology has the same functional benefits (e.g. speed, in-house cheapness, irreversibility) that would be advantageous for the operation of any kind of monetary systems.

However, it is not yet clear what could be the real functions of the VCS. One of these could be to renew or reshape the payment system, but it requires moderate volatility and minimal exchange rate fluctuations. Many see VCS as an investment opportunity despite of the obvious and less obvious risks.

Looking back to the basic assumptions (Tibor Nagy) that money is originally independent from the state as it is created in a spontaneous development; the state regulates it due to different considerations (Istvan Simon); and considering Samuelson's and Nordhaus's money paradox[18] that money is accepted because it's accepted, then we should classify VCs as money. We should consider these means as money because they developed spontaneously, and there are people around the world (even if still not in majority) who accept it as a means of payment.

As we can see in the development of money, there is recently no other widely-used, accepted currency in the world than the currencies issued and regulated by a state or group of states (e.g. Eurozone Member States). Currencies became official currencies of any states by regulation. Looking back in history, a relatively long time ago each currency had a "host or owner/issuer state" that solely regulates the issuance and the functioning of its currency and own monetary system.

The emergence of virtual money, virtual currencies have disturbed this long-standing world-wide social convention since we suddenly have to face the existence of these new kind of money that some people accept even if they do not have a "host/owner" state regulating system and issuance. Question is whether what consequences should be drawn for regulation of virtual currencies and their markets? Should the states of the world allow the emergence of an alternative monetary system (s) along the traditional ones?

Virtual currencies are a kind of criticism on the traditional monetary systems. We must also see, however, that this criticism erodes one of the basic elements of state sovereignty, the financial sovereignty, including the right to issue the own currency.[19]. Ernő Várnay has highlighted two specific rights of the state related to the monetary sovereignty: the right to determine the official currency on its territory and the right to determine

[18] P. A. Samuelson and W. Nordhaus, *Közgazdaságtan I*. (KJK 1990) 386.
[19] Cf. Bodin's concept on soveregnty (n 8).

the rules applicable on the currency exchange.[20]. Interestingly, central banks of Europe, US, Canada don't see the appearance and development of the VCs as threat on the traditional monetary system. Central banks issue only notices on the risks of usage of VCs.

4. Virtual currencies as systemic risks

Before the appearance of the VCs the monetary system of the world was homogeneous: almost each sovereign state (either alone or together with others) had its own currency, and each monetary system was regulated by a state. This global regulation provided the possibility of state (central bank) intervention through monetary control and the central banks were anyhow liable for their decisions. An essential issue is that by the emergence of the virtual currencies – especially in case if the capitalization and the significance of them compared to the current levels gains more importance, states and central banks may lose control over financial and monetary systems and processes (or at least their control capacity may weaken substantially). Another issue could be that if a substantial amount of liquidity flows from traditional currencies to VCs, this can have a negative effect on the situation of the traditional banking sector. VCs are outside the scope of the central bank's monetary policy toolbox, and therefore neither the central bank's interest rate policy (virtual assets is conceptually interest-free) nor the exchange rate policy can have any impact.

In my view, in the light of this background, the national states of the world cannot afford to ignore this issue and not provide an adequate regulatory response within the foreseeable future in order to stabilize the monetary system of the world. The question is, however, whether it is possible to adopt any effective regulation beyond the prohibition, and what can be regulated?

As a first step, the regulator definitely has to focus on *payment function of the VCs*. In this area, it is necessary to define transactions which can be implemented by a virtual currency. In my view for example the *payment of taxes* and other state revenues in will not be possible in

[20] Ernő Várnay, 'Költségvetési és monetáris szuverenitás az Európai Unióban' Pro Publico Bono – Magyar Közigazgatás (2013) (1) 26-59., and Ernő Várnay, 'A fiskális és a monetáris szuverenitás az Európai Unióban – az Európai Unió alkotmányos szerződésére is figyelemmel' in István Simon (ed), *Tanulmányok Nagy Tibor tiszteletére* (Szent István Társulat 2009) 295–309.

the foreseeable future in other currency than the one issued by the respective national state. Waiving taxation on own currency would practically mean waiving and cessation of own currency either. This restriction is a serious constraint itself for the conversion of all other transactions into VC, since the conversion of "market" transactions to VCs immediately involves a significant exchange rate risk for merchants, service providers and other taxpayers, as well for the states themselves collecting taxes in VCs. One of the first experiments is the attempt of US State of Ohio, however it is not a real VC payment. The treasurer's office doesn't have a bitcoin account. When a business pays in bitcoin, that payment is routed through an intermediary company, which converts the bitcoin into USD, which then get sent to the tax office. This method of tax payment didn't proof a huge success. According to press reports[21] citing Ohio treasurer's office fewer than 10 companies had used the option. Beside Ohio, there are pilot projects in the Switzerland (in canton Zug and in the municipality of Chiasso).

In the light of the above-mentioned circumstances, it does not appear necessary to introduce limitations on market transactions and private parties related to the usage a VCs instead of using their traditional currency (similarly as it is possible to use different traditional currencies). The task of the states and central banks to draw the attention of the users on the risk related the volatility of the exchange rates. Prohibitions and restrictions should only be considered if the stability of the monetary and financial system was compromised, or specific legal interests are to be defended like the value of wages. However, *payment of wages* in VCs raise specific issues. Wage payment in cryptocurrency makes it convenient to hire remote workers globally since payments can be made almost instantly and around the globe, even without access to the local banking institutions. On the other hand, beside the possible significant exchange rate fluctuation and related risks, there are legal issues employers and employees have to face with. Firstly, for the reason of defence of wages, several jurisdictions require the payments of wages in local currency[22],

[21] <https://www.marketplace.org/2019/04/08/ohio-experiments-bitcoin-tax-payments/>

[22] This is the case for example in Hungary either. Cf. Art 154 of Act I of 2012 on the Labour Code.

but in some countries (e.g. New Zealand[23]) it is already allowed to pay in VCs. Factually, there are further countries (Japan, Australia, Denmark), where employers can pay wages – in lack of legal regulation and/or at least partially – in cryptocurrencies. Although, VC payments – even salary payments – can be used globally, one has to keep in mind that taxation of these assets and payments differs country by country. Furthermore, a remarkable constraint can be the different nature of certain VCs, namely whether they are to be regarded as securities or not. The Securities and Exchange Commission ("SEC") of the USA has taken the stand that since the value of any given cryptocurrency may appreciate due to the efforts of third parties, it is as good as a speculative instrument and therefore must be regulated as such[24]. In case of payment salaries in VCs, there are also differences between two situations: (1) salaries defined and contracted in fiat currency and changed (on choice of the employee as fringe benefit) to VC before payment, (2) salaries defined and contracted in VC. The second option has not been really wide-spread yet.

As a second step, it is necessary to examine whether the *lending/borrowing activities* in in VCs can allowed. In fact, VC lending services are already existing[25]. VCs can be simple means of P2P lending platforms. In case of P2P platforms, no bank type intermediary institution is needed, the platform itself connects the creditor and the borrower. For proper creditor and borrower protection P2P platforms would need special regulation – independently from the type of currencies (fiat or virtual) they use for operation.

To illustrate the risks of this issue on both creditor and borrower side, it is perhaps enough to mention the FX-based lending, which resulted the most serious domestic financial disaster of the last two decades in Hungary. It may only be allowed if and when the incomes of the borrowers involved are predominantly originating in virtual currency. Until that happens, this activity must be definitely restricted.

[23] Cf. 'New Zealand legalises salaries paid in cryptocurrencies' (Financial Times, 12 August 2019) <https://www.ft.com/content/54dd4854-bd06-11e9-b350-db00d509634e>.

[24] Cf. SEC President Clayton's statement at <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>.

[25] E.g. <www.ethlend.io>.

A related question is the *VC backed lending*. Even currently lending services backed by VC assets are also available[26]. These operations are less risky than VC lending, however the fluctuation of rates may make additional coverage necessary.

As a third step, it is necessary to examine whether virtual currency can be considered as a *financial instrument* serving as an investment target. Applicable regulations[27] do not even consider traditional currencies as a financial instrument, as a subject of investment services. Virtual currencies don't pay interest or dividends. Financial benefits, returns on them can only arise from their exchange rate fluctuations. However, this is known to show significant shifts. With regard to traditional convertible currencies, the convertibility and the financial gains arising from the exchange rate changes are not restricted and the gains are not subject of income tax in the case of private individuals (in Hungary). There is no apparent reason for any restriction on the conversion or redemption of traditional currency into a virtual currency or vice versa, even if it is for any gainful purpose. Prohibitions and restrictions here are only to be considered if the stability of the financial system is compromised.

Fourthly, it would be necessary to have a look at the current regulatory environment of the service providers and their operation, who provide currency exchange services related to virtual currencies. The EU bank regulations[28] and the Hungarian Credit Institutions Act[29] define currency exchange as an auxiliary financial service provided by a bank (and by its agent).

However, by definition foreign exchange transactions (and services) mean only the sale of foreign currency (money issued by a foreign state/central bank) against a domestic or foreign currency and vice versa. The sale/exchange of virtual currencies against traditional (foreign or

[26] Cf. <www.saltlending.com>.

[27] Directive 2014/65/EU of the European Parliament and of The Council on markets in financial instruments (MIFID II) [2014] OJ L173/349, Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities (Hungary).

[28] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD) [2013] OJ L176/338, Regulation No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms (CRR) [2013] OJ L176/1.

[29] Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (Hungary).

domestic) currency is outside the concept of currency exchange service and as such does not fall under the scope of the Credit Institutions Act. Consequently, this activity doesn't require the authorization by the financial supervisory authority and neither supervised by it. The regulation of this activity is possible and justified in line with the traditional currency exchange services, especially if we consider that the unregulated trade of these instruments can be a simple tool for covering of various illicit activities or criminal offenses and/or the gains originating from them. In lack of legal regulation and protection, the operation of VC trading platforms and wallet service providers can carry serious security risks. As many examples show their possible malfunction, bankruptcy, or technical failure causing serious and irreversible damage for VC owners.

In further steps, it is necessary to examine the impact of the use of VCs on the implementation different financial transactions. Here, inter alia, the applicability of various law enforcement measures (e.g. enforceability of claims, administrative decisions, court rulings) may become at least questionable. For law enforcement authorities the legal regulation technically cannot provide such an easy access to VC storage facilities (e.g. wallets) as to a traditional bank account. For example, in the case of Bitcoin, the owner's access to his/her wallet can be limited by law enforcement and/or forensic measure, but the success of the coercive measures depends in many cases on the owner's willingness to cooperate. [30] In case of other, yet less popular VCs like Monero, Zcash the identifying and tracking of the owner is much more complicated or even told as impossible.

Finally, I consider as a basic question to take substantive steps as soon as possible in order to prevent money laundering and other criminal offenses by usage of virtual currencies. This problem persists until, for example, the Bitcoin transactions themselves can be tracked but the identification of the parties involved remains insufficient.

5. Conclusions

We have seen the fundamental question related to the effective functioning of the current financial and legal system is not whether it is necessary to regulate the VCs (both their issuance and usage), but all the more how can this be achieved and furthermore how can we ensure the

[30] Cf. Zoltán Szathmáry, 'Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban' (2015) (11) Magyar Jog, 639.

proper operation and of our monetary, financial and also legal system in case of a surely occurring further proliferation of the VCs? The usage of VCs cannot be abolished. Taking down any computers of the P2P network have very limited effect on the whole system. Any legal prohibition would unlikely stop VC usage since one's identity on the network is almost untraceable. The first possible step could be the regulation and monitoring of the traditional/virtual currency exchange/intermediary activities (not solely AML) – by transnational or rather global regulatory measures. Local or regional regulations don't worth a single Bitcoin.

At the time of writing of this study, there are no Hungarian and EU laws in force regulating this subject in general and neither any regulatory measures are there in at least that areas of it having the highest risks due to the non-regulation. In July 2016, the European Commission has tabled a proposal on the amendment of the Anti-Money Laundering (AML) Directive[31] ,, proposing the list of so-called obliged entities defined by the Directive to be complemented by virtual exchange platforms and custodian wallet providers. The proposal also includes a definition of the term "virtual currency"[32]. The proposal aims to counterbalance the anonymity related to the VC transactions in comparison with traditional currency transfers, with particular emphasis on the fact that public administrations (in and outside EU) are currently not monitoring the payments in VCs. The proposal has been approved the Council and the European Parliament after 2 years of discussion in May 2018[33] Once came into force and will be transpositioned by 10 January 2020, the Directive affects only one element of the issues raised.

Right now, in the world of the Internet, the state can determine its own currency, its usage in taxation and obligatory acceptance, however the

[31] Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/ECCOM(2016) 450 final.

[32] "Virtual currencies" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

[33] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

state cannot ensure its exclusivity either. Although the regulation of creation or issuance of VCs is practically impossible, it may be easier to regulate the access to them and the exchange transactions especially between the traditional and the virtual currencies.

The task, therefore, is not simple but requires a global regulatory response. The bitcoin.org page itself points out that "the Bitcoin protocol itself cannot be modified without the cooperation of nearly all its users, who choose what software they use. Attempting to assign special rights to a local authority in the rules of the global Bitcoin network is not a practical possibility". the situation can be even more complicated by the creation and use of further less well-known virtual currencies that might also help illicit purposes.

The VC schemes as whole cannot be regulated effectively. The regulation can focus on the activities (e.g. exchange services) and the intermediaries. However, the regulation cannot cover the whole scheme due to the lack of central authority controlling the system. If once exchange services were not needed anymore due to the spread of any VC, the regulation was even more extremely difficult.

In addition to the necessity of regulation, a further question is whether the blockchain system underlying the operation of the VCs can be adapted to the development of the traditional financial system? Since this new technology has undoubted advantages either, and it cannot be ruled out that a VC operating without the above-mentioned issues might emerge in the future, the state and central bank decision-makers should it consider in the development and regulation of the financial system.

References

- Bodin, Jean, *Six books on the Commonwealth*, Chapter X: The true attributes of sovereinty
- European Banking Authority, 'EBA Opinion on 'virtual currencies'' (4 July 2014) EBA/Op/2014/08
- European Central Bank, 'Virtual Currency Schemes – further analysis' (February 2015)
- Financial Times, ' New Zealand legalises salaries paid in cryptocurrencies' (12 August 2019) < https://www.ft.com/content/54dd4854-bd06-11e9-b350-db00d509634e >

- Halász, Zsolt, 'Public Finances' in Varga, András Zs., Patyi, András and Schanda, Balázs, *The Basic (Fundamnetal) Law of Hungary – A Commentary of the new Hungarian Constitution* (Clarus Press 2015) 321-343
- Hayek, Friedrich August, *Denationalisation of Money* (Institute of Economic Affairs 1976)
- Hileman, Garrick and Rauchs, Michael, 'Global Cryptocurrency Benchmark Study 2017' (University of Cambridge)
- Ma, Adrian, 'Ohio experiments with bitcoin tax payments' (8 April 2019) <www.marketplace.org/2019/04/08/ohio-experiments-bitcoin-tax-payments/>
- Marx, Karl. *Das Kapital*: *Kritik der politischen Öekonomie* (first edition, Verlag von Otto Meissner 1867)
- Nagy, Tibor, 'A pénzrendszer joga' in István Simon (ed) Pénzügyi Jog I. (Osiris 2007) 275
- P. A. Samuelson and W. Nordhaus, *Közgazdaságtan I*. (KJK 1990) 386
- István Simon, 'Állandóság és változás a pénz jogi szabályozásában' in: István Simon (ed) *Tanulmányok Nagy Tibor tiszteletére* (Szent István Társulat 2009)
- Szathmáry, Zoltán, 'Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban' (2015) (11) Magyar Jog, 639
- Várnay, Ernő, 'Költségvetési és monetáris szuverenitás az Európai Unióban' Pro Publico Bono – Magyar Közigazgatás (2013) (1) 26-59
- Várnay, Ernő, 'A fiskális és a monetáris szuverenitás az Európai Unióban – az Európai Unió alkotmányos szerződésére is figyelemmel' in István Simon (ed), *Tanulmányok Nagy Tibor tiszteletére* (Szent István Társulat 2009) 295–309
- Vígvári, András, *Pénzügy(rendszer)tan* (Akadémiai Kiadó 2008)
- Weber, Max, *Wirtschaft und Gesellschaft* (Mohr 1922)

Short biography of the author

Zsolt Halász was born in 1977 in Budapest, Hungary. He is graduated from Péter Pázmány Catholic University Faculty of Law and Political Sciences, Budapest, Hungary in 2000. He holds LL.M. from the same

university (2002) and PhD from the University of Miskolc (Hungary), Faculty of Law (2011). In 2001-02 lawyer in the CEO's Office of the Hungarian Development Bank. 2002-2005 in house lawyer in the Hungarian Investment and Asset Management Ltd. 2005-10 legal referent in the Office of Parliamentary Commissioner for Human Rights (Ombudsman). 2010-13 director and head of CEO's Office in the Hungarian Development Bank. 2013-16 advisor to the Vice-President of the European Investment Bank (EIB), 2016-18 policy officer at EIB. Since his graduation he has been continuously teaching financial law at Péter Pázmány Catholic University Faculty of Law and Political Sciences and in 2018 he has been appointed to associate professor and head of the Financial Law Department of the University.

The Classification of Virtual Currencies Related to Blockchains

Péter Bálint Király*

Abstract: In the 21. century there is an increasing number of digital or virtual assets, that have some kind of value. We use different names for these assets, and countries have different definitions for those names. Among these there are virtual currency, digital currency, cryptocurrencies, security and utility tokens, and so on. As these assets are digital or virtual, and are existing on the internet, they can be used globally. That is why regulators should come up with a unified definitions and terminology. In my presentation and paper I will present what is considered to be a virtual currency. I also try to answer the question what are the cryptocurrencies and other digital tokens that are generated in a blockchain system, and whether they can be seen as a kind of virtual currency.

Keywords: blockchain, cryptocurrencies, virtual currencies, tokens

1. Introduction

Over the last few years, we have heard a lot about FinTech in the television on the Internet. The term refers to an active relationship between financial services and IT development, in which either new e-services are created or existing financial services are further developed by electronic, digital devices. Fintech is one of the umbrella terms of financial developments in the 21st century.[1] Out of the Fintech innovations, in this paper I will introduce the definition of the blockchains and their associated tokens, ie, cryptocurrencies, security, utility and asset tokens.

Supported by the ÚNKP-18-3 New National Excellence Program of the Ministry of Human Capacities

* PhD student, Széchenyi István University, Faculty of Law, Department of Administrative and Financial Law (Győr), kiralypeterbalint@gmail.com

[1] Patrick Schueffel, 'Taming the Beast: A Scientific Definition of Fintech' (2016) 4 (4) Journal of Innovation Management <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097312> accessed 4 March 2019, 32-54.

We encounter a typical problem when we want to deal with the legal analysis of blockchains and related technologies: the technical description of the technology and its economic analysis is much more advanced than the legal studies about the topic. Cryptocurrencies, as an element of the phenomenon, are already present in the legal literature,[2] but those who are interested in blockchains and other types of tokens typically get their information about them through blogs and thematic forums. In 2015, the Central Bank of Hungary drew attention to the dangers of new technologies,[3] but the legislator did not take a substantive position on the relevant issues: Can they be consider as currencies? Or are they securities, maybe commodities? In the following, I am looking for the answer to these questions of how can we categories the different tokens using the existing legal framework.

2. What are the blockchains and tokens?

Here are two basic definitions that need to be clarified: blockchains and tokens. I consider it important to explain the concepts, because without knowing the definitions it is not possible to continue a substantive discourse on the subject. In addition, I want to clarify the common misbelief that BitCoin, cryptocurrencies and blockchains are synonymous terms. However they are not the same.

By many blockchains are already considered the most important invention of the 21st century, and they say it can change the world in a similar way the internet did. The blockchain is a peer-to-peer protocol, a network of which anyone can join, can initiate transactions and authenticate them by creating so-called blocks. Blockchain is essentially a distributed or decentralized ledger, which is public and thanks to cryptographic procedures validates the recorded data (for example, transactions) credibly in an unalterable manner without any intermediary.[4]

[2] Ádám Kerényi and Júlia Molnár, 'A FinTech-jelenség hatása – Radikális változás zajlik a pénzügyi szektorban?' (2017) 16 (3) Hitelintézeti Szemle, 32–50.

[3] Central Bank of Hungary, 'Sajtóközlemény: Újabb kockázatok a fizetésre használható virtuális eszközök körében' (2015) <https://www.mnb.hu/felugyelet/felugyeleti-keretrendszer/felugyeleti-hirek/hirek-ujdonsagok/sajtokozlemeny-ujabb-kockazatok-a-fizetesre-hasznalhato-virtualis-eszkozok-koreben> accessed 28 October 2018.

[4] Primavera De Filipp and Aaron Wright, Blockchain and the Law: The Rule of Code (Harvard University Press 2018) 13-14.

How does it work? In case of BitCoin (the very first cryptocurrency) information about the transactions are gathered and bundled up in so-called blocks every 10 minutes.[5] The transactions in the new block are then authenticated and verified by the computers of the blockchain system, e.g. confirm that the buyer actually had the amount of cryptocurrency at his disposal. Then, the so-called header of the previous block is also added to the data series of the new block. This headset practically works like a personal identification number. Each block has a unique header, through which it can be identified. This means that each block refers to the previous block, consequently, the chain of transactions can be traced back to the original block of the very first transactions. Once the header of the previous block has been added to the new block, encryption of the data in it will begin by deciphering a cryptographic puzzle.[6] All computers that run the block chain are competing to solve the cryptographic puzzle as soon as possible, because whoever first solves the puzzle gets rewarded with BitCoin (or in case of another blockchain with some other kind of cryptocurrency) for their work. This process is called "mining" in the internet slang and this is the way to get Bitcoin or other cryptocurrency without real money.[7] (Nowadays you can buy cryptocurrencies with real money in a way similar to currency exchange. In addition, BitCoin and other cryptocurrencies are also listed on the stock market.)[8] The verified new block will be the proof of work. The thus-authenticated block is then provided with a time stamp and then added to the blockchain's previous blocks in a chronological order.[9]

The blockchain contains all transactions that have ever been executed by using it. The entire blockchain is constantly updated, and it can be

[5] Mayukh Mukhopadhyay, *Ethereum Smart Contract Development - Build Blockchain-based Decentralized Applications Using Solidity* (Pact Publishing 2018) 15-18.

[6] Daniel Drescher, *Blockchain Basics – A Non-technical Introduction in 25 Steps* (Apress 2017) 23.

[7] Adam Hayes, 'What factors give cryptocurrencies their value: An empirical analysis' (2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579445> accessed 13 October 2018, 2.

[8] Jonathan Chiu and Thorsten V. Koeppl, 'The Economics of Cryptocurrencies – Bitcoin and Beyond' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048124> accessed 28 March 2019, 1-5.

[9] Hayes (n 7) 2.

found on all participating computers. Thus, all computers are capable of proving that a certain transaction is completed, and who is the current and former owner of a particular product or money.[10] It is also safe because the transactions are practically unchangeable and unhackable after being added to the blockchain. In order for a hacker to change a transaction, it is necessary to modify not only the block of the transaction in question, but also the data of the preceding and subsequent blocks, as they are all linked together. In addition, they need to do hack all of (up to millions) the nodes' computers, because all of them store the whole blockchain. In addition, thanks to consensus models, nodes benefit more if they are involved in the operation of the system, in maintaining its safety and reliability, than hacking the blockchain.[11]

Different tokens may be associated with the operation of the blockchains. The tokens are fungible and negotiable assets, which has financial value or represents a right, and what is recorded on a blockchain.[12] Four types of tokens can be distinguished:

a) Utility tokens: embody the right to access a future service or product (usually a blockchain).
b) Security tokens: embody the ownership of an investment asset or other intangible asset.
c) Asset tokens: embody the ownership share of a movable or real estate thing.
d) Cryptocurrencies: assets, that are aaccepted and used as an exchange or payment instrument. They are issued not by a central bank, but by a developer / developer team.[13]

[10] Hossein Kakavand, Nicolette Kost De Sevres and Bart Chilton, 'The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251> accessed 5 November 2018, 4-5.

[11] Sarah Wurfel, 'Blockchain is unhackable but these are 5 possible vulnerabilities of "the new Internet"' (2018) <https://captainaltcoin.com/blockchain-hacks/> accessed 13 Januar 2019.

[12] Jonathan Rohr and Aaron Wright, 'Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets' (2017) Cardozo Legal Studies Research Paper, No. 527 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104> accessed 21 April 2019, 17-20.

[13] Ferdinando M. Ametrano, 'Hayek Money: The Cryptocurrency Price Stability Solution' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270> accessed 10 December 2018.

The distinction between the above categories can be difficult, as there is only a thin line between them, and one can transform into another.

3. The issue and functions of tokens

The purpose of creating cryptocurrencies was to create a virtual currency which functions like real money, with the difference that in the case of Bitcoin there is no need for an intermediary institution (e.g. bank) for the execution of transactions. The system thus provides direct (peer-to-peer), faster, cheaper and safer financial transactions. The traditional bank transfer is slow (especially if we want to transfer money to a foreign bank account) and comes with a lot of administrative tasks. In addition, a third party's (financial institution's) contributuion is necessary, who monitors and executes the transfers, which will incur additional costs. The banking system is vulnerable to fraud and cyberattacks, and the possibility of human error can not be excluded. Cryptocurrencies address these problems with introduction of the blockchain technology. [14]

Among the blockchains there are those in which the release of cryptocurrencies is continuous, since the participants in its operation receive newly issued cryptocurrency units in return for their contribution to the authentication of transactions as a compensation or reward. This process is called mining.[15] Continuously issued cryptocurrencies include those that have an upper limit on their quantity, while others can be issued in unlimited quantities. In addition, there are also block chains in which the amount of cryptocurrency associated with it is predetermined and issued at once during its establishment, and its amount does not change later. In these cases, a transaction fee is paid for the miners as a reward for their work in authentication of transactions. The function of the cryptocurrencies is twofold: on the one hand, they serve as a means of exchange (currency) and on the other hand they play an incentive role in the blockchain system. The cryptocurrencies themselves have no value. They only gain value, because they are accepted as a means of exchange within the users of a blockchain.

[14] Don Tapscott and Alex Tapscott, *Blockchain Revolution: Hot the Technology Behind Bitcoin is Changing Money, Business and the World* (Portfolio Penguin 2016) 55-59.

[15] Hayes (n 7) 2.

In contrast security, utility and asset tokens don't have inherent value, they only have value because they represent some valuables or rights.[16] Both security and utility tokens are issued in a predetermined number.[17] In addition utility tokens can only be used once, as they are „burned" after they are redeemed. Exactly what kind of rights a token owner has is different case by case. These permissions determine whether it is a security, utility or asset token. Security and utility tokens are issued through the process of the so-called Initial Coin Offering (hereafter ICO). ICOs are essentially a form of fund raising, when we create a new blockchain, and the amount of money needed to set up the system associated with it is offered to us by others usually in cryptocurrencies like BitCoin or Ether, or in legal tenders.[18] In this sense they work as a tool for crowdfunding. The essence of this is that an external financial resource can be collected without the use of any intermediary, since the collection of money is handled through the blockchain system. Usually when someone wants to create a new blockchain they turn to the public for monetary support. The founders offer tokens for those who give them money for the establishment of a blockchain. The entrepreneur thus gets the money to start the business, while the contributor acquires a token that embodies their rights in the future blockchain system. Its advantages are that it is a token that can be sold at any time and therefore has a high level of liquidity.[19] Furthermore, there is practically no transaction costs and is available to potential investors at a global level, and because of

[16] Dirk A. Zetzsche et al., 'The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators' (2017): (2017) University of Luxembourg Law Working Paper, No. 11/2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298> accessed 7 December 2018, 8-9.

[17] Vlad Burilov, 'Utility Token Offerings and Crypto Exchange Listings: how regulation can help?' (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3284049> accessed 16 March 2019.

[18] Theodoros Stylianou, 'An Investigation into the Utility and Potential Regulation of Initial Coin Offerings and Smart Contracts in Selected Industries and Jurisdictions' (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3276822> accessed 16 March 2019, 9-10.

[19] Stylianou (n 18) 9-10. o.

unregulated nature of the phenomenon, it also entails fewer legal obligations than the initial public offering.[20]

So what is the connection between tokens and blockchains? Blockchains register and record the transfer of tokens. As I already mentioned blockchain is a basically a ledger, and its main purpose is to create a way to transfer value without any intermediary like banks, in a cheaper, faster and safer way. Through the tokens, the team of developers of the blockchain can also obtain financial resources for the operation of their project. The tokens are also a reward for contributing to the operation of the block chain, as the „miners" receive tokens for their contribution in the operation of the blockchain system.[21]

4. The legal classification of tokens

Are these tokens considered to be money, or investment or commodity? As long as it remains a question, token holders will always refer to the version that is more appropriate for them. Today countries have different solutions, and sometimes even different authorities in a given state interpret tokens differently.

Tokens can be seen as currency. In the economic sense in order to be considered currency, it needs to have the following three functions: a) a store of value, b) a means of exchange and c) a unit of account.[22]

The store of value function is met if the thing can reliably keep its purchasing power for a long period of time. Some authors say that due to frequent changes in the value of tokens compared to other currencies, it is unable to function as a store of value. However, according to the European Central Bank the frequent and significant changes in value does

[20] Philip Stastny, 'Underpricing Effects in ICOs' (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3206323> accessed 16 March 2019, 1-2.

[21] Judit Glavanits and Péter Bálint Király, 'A blockchain-technológia alkalmazásának jogi előkérdései: a fogalmi keretek pontosításának szükségessége' (2018) (3) Jog – Állam – Politika.

[22] István Gárdos, 'A pénz fogalma' (2016) (1) Polgári Jog <https://gmtlegal.hu/cikkek/a-penz-fogalma.php?kid=4&did=273> accessed 11 October 2018, 1.

not affect the ability to preserve the value, since all legal tenders are subject to such changes.[23]

The medium of exchange function is fullfilled if something „passes freely from hand to hand troughout the community in final discharge of debts and full payment of commodities, being accpeted equally without reference to the character or credit of the person who offers it and without the intention of the person who receives it to consume it or apply it to any other use than in turn to tender it to others in discharge or debts or payment for commodities. Tokens, mainly cryptocurrencies comply with this condition, since it was originally created for this purpose, plus they are actually being accepted as counterparties for various transactions in increasing numbers.[24]

The unit of account function means that the value of goods and services can be expressed in the subject matter. This may actually be true of any thing as is shown in history (e.g. gold, shells, etc. were used as money). Tokens are in principle capable of fulfilling this function, but most of the time we see that the price of products is determined in dollars, euros or other currencies beside e.g. BitCoin.[25]

So cryptocurrencies meet the requirements to be considered money in the economic sense. In legal sense, however, we can only speak of legal tender, if the money was issued by a central bank or other monetary authority of a State.[26] Cryptocurrencies are not currencies, because it is not issued by a central bank. [27]

Tokens can also be interpreted as investment, because of the constant and large changes in their value. Consequently, it is more like a speculative investment instrument, especially if we add that there are some who just buy e.g. BitCoin in order to later sell it, and thus gain profit.

[23] Antonio Madeira, 'How legal is Bitcoin and Crypto Currencies?' (2015) <https://www.cryptocompare.com/coins/guides/how-legal-is-bitcoin-and-crypto-currencies/> accessed 23 November 2018.

[24] Wiliam J. Luther and Lawrence H. White, 'Can Bitcoin Become a Major Currency?' (2014) George Mason University Working Paper in Economics, No. 14-17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446604> accessed 12 February 2019, 1-6.

[25] Stephanie Lo and J. Christina Wang, 'Bitcoin as Money?' (2014) (4) Federal Reserve Bank of Boston Current Policy Perspective <https://www.bostonfed.org/publications/current-policy-perspectives/2014/bitcoin-as-money.aspx> accessed 19 November 2018, 3-4.

[26] Ametrano (n 13).

[27] Luther and White (n 24) 1-6. o.

However, high volatility can easily discourage investors. Also it is easy to see the resemblance to investments in the case of security tokens. In case of ICOs we can say that, they are similar to the Initial Public Offering (IPO). The question is whether this way of financing can be considered as a security? According to the U.S. Securities and Exchange Commission (SEC): „the federal securities laws apply to those who offer and sell securities in the United States, regardless whether the issuing entity is a traditional company or a decentralized autonomous organization, regardless whether those securities are purchased using U.S. dollars or virtual currencies, and regardless whether they are distributed in certificated form or through distributed ledger technology."

The SEC based its decision on the Howey test, according to which a contract is qualified as investment contract, if there is an investment of money, there is an expectation of profits from the investment, the investment of money is in a common enterprise, and any profit comes from the efforts of a promoter or third party.[28] If someone buys cryptocurrency for the purpose of gaining profit later on by selling them, then the first two conditions are fulfilled (however it is still a question whether somebody bought the BitCoin in order to sell them later). The joint venture element is also accomplished as the transaction executed through the blockchain network contributes to the investor's growth, and the position of investors is affected by the appreciation or depreciation of the cryptocurrency. The last condition is also met if miners are considered to be third parties or promoters and the invertor's profit is a consequence of the miners activity.[29] Interestingly, according to the same statement of the SEC, Ether is not qualified as an ICO, but as virtual currency,[30] from which it follows that the authority makes a distinction between investment-like cryptocurrencies and money-like cryptocurrencies. Therefore, if a cryptocurrency can prove that it at least one of the

[28] Securities and Exchange Commission, 'SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities' (2017) < https://www.sec.gov/news/press-release/2017-131> accessed 19 November 2018.

[29] Tara Mandje, 'Bitcoin, its Legal Classification and its Regulatory Framework' (2015) 15 (2) Journal of Business & Securities Law <https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1003&context=jbsl > 172-178.

[30] Securities and Exchange Commission (n 28).

conditions is not met, then it will not qualify as a security.[31] However, it should be noted that not all cryptocurrencies based on mining (e. g. the ones that use the Proof of Stake consensus method).

Furthermore according to SEC a token can transition from being a security token into a cryptocurrency, and thus it cannot be considered as a security anymore, because once the blockchain is established, and the value of the token is no more based on the efforts of third parties. But there are two problems with this phenomenon: a) when can we say that a given token is ceased to be a security; b) in case of cryptocurrencies their is always based on the efforts of a promoter or third party, ie. miners.[32]

Tokens can be considered as commodity, because of their resemblance to gold. Gold and tokens both have: a) finite supply (BitCoin allows the mining of 21 million Bitcoin in total), b) none of them is supervised by a single government, c) the value of both are determined by demand and supply. But these statements are not true for all tokens.[33] Some cryptocurrencies can have be mined in unlimited amounts (e.g. DogeCoin). Some have a predetermined amount available since their establishment (e.g. Ether). However asset tokens (even though they are not really similar to gold) could be seen as commodity, because they represent real life commodities,[34]

5. The solution

In my opinion there are two preliminary questions that need to be clarified before we can categorize cryptocurrencies.

1. Can we list every token into the same category? As we saw earlier, cryptocurrencies are considered as commodities because of their

[31] Marinoff, Nick, 'SEC Chairman: Cryptocurrencies Like Bitcoin Are Not Securities, but Most ICOs Are' (2018) <https://bitcoinmagazine.com/articles/sec-chairman-cryptocurrencies-bitcoin-are-not-securities-most-icos-are/> accessed 11 April 2019.

[32] James J. Park, 'When Are Tokens Securities? Some Questions from the Perplexed' (2018) UCLA School of Law, Law-Econ Research Paper, No. 18-13 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298965> accessed 16 March 2019.

[33] Evan Faggart, 'What Happens to Bitcoin Miners When all Coins are Mined?' (2015) <https://news.bitcoin.com/what-happens-bitcoin-miners-all-coins-mined/> accessed 17 October 2018.

[34] Margaret Nail, 'How infinite are cryptocurrencies?' (2017) <https://bitnewstoday.com/market/mining/how-infinite-are-cryptocurrencies/> accessed 12 February 2019.

resemblance to gold, because both of them is finite in number, and demand and supply affect their value. However, this argument is not true for all cryptocurrencies, not to mention security, utility and asset tokens, since, as I have already mentioned, some of them have unlimited amounts available, or those that already have a limited amount in the system from the beginning.

2. Can we list a single token, e.g. BitCoin into only one category? This question arise from the fact, that Bitcoin can be used as money, as an investment, and as a commodity as well. But if that is the case, then legal acts for all the three categories should be applied, which can very easily lead to over-regulation, which would hinder the development and use of cryptocurrencies, although it is an extremely useful and versatile invention.

In conclusion we saw that the classification of tokens is not easy to do, as legal framework in effort is not suitable to them. So what can be a solution here. In my opinion we need to come up with an umbrella category that covers all of these tokens. I think the most ideal candidate for this task is the category of virtual currencies. There is no exact definition of virtual currencies. According to the Financial Action Task Force: Virtual currency is a digital representation of value that can be digitally traded and functions as a medium of exchange; and/or a unit of account; and/or a store of value, but does not have legal tender status in any jurisdiction.[35] However the European Central Bank use the term virtual currency with the following meaning: a virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community. Both of them consider cryptocurrencies to be virtual currencies, and in my opinion we can also see security, utility and asset tokens as such.[36]

In conclusion it is likely that in the near future none of the blockchain related tokens will accepted as legal tenders by most countries, because – among other reasons – it would jeopardise the money-issuing monopoly

[35] Financial Action Task Force, 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' (2014) <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 3 December 2018, 4-5.

[36] European Central Bank, 'Virtual Currency Schemes' (2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 28 November 2018, 13.

of states. Moreover, their interpretation as an investment and a commodity is also not certain, as it was explained above. The legal consequences (such as taxation, consumer protection, etc.) are based on the classification, so it should be the priority of legislation to answer this question. Tokens cannot remain unregulated due to their growing importance, therefore, it is much more likely that states will regulate them in some way. The question is merely what the regulation will be. In my view, the most important thing to do is to create uniform regulation. This would be extremely beneficial because token are a virtual asset that are available through the internet at anywhere and anytime around the world, and it can be exchanged regardless of borders. In my opinion, the process launched by BitCoin and other cryptocurrencies is irreversible. That is why it would be necessary to agree whether tokens are a currencies, a commodities or an investments, or to come up with a new category (like virtual currencies) that cover all tokens. It is essential since a single regulation would ensure that we can take advantage of the economic opportunities inherent in tokens much more easier.

References

- Ametrano, Ferdinando M., 'Hayek Money: The Cryptocurrency Price Stability Solution' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270> accessed 10 December 2018
- Burilov, Vlad, 'Utility Token Offerings and Crypto Exchange Listings: how regulation can help?' (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3284049> accessed 16 March 2019
- Central Bank of Hungary, 'Sajtóközlemény: Újabb kockázatok a fizetésre használható virtuális eszközök körében' (2015) <https://www.mnb.hu/felugyelet/felugyeleti-keretrendszer/felugyeleti-hirek/hirek-ujdonsagok/sajtokozlemeny-ujabb-kockazatok-a-fizetesre-hasznalhato-virtualis-eszkozok-koreben> accessed 28 October 2018
- Chiu, Jonathan and Koeppl, Thorsten V., 'The Economics of Cryptocurrencies – Bitcoin and Beyond' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048124> accessed 28 March 2019

- De Filippi, Primavera and Wright, Aaron, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018)
- Drescher, Daniel, *Blockchain Basics – A Non-technical Introduction in 25 Steps* (Apress 2017)
- European Central Bank, 'Virtual Currency Schemes' (2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 28 November 2018
- Faggart, Evan, 'What Happens to Bitcoin Miners When all Coins are Mined?' (2015) <https://news.bitcoin.com/what-happens-bitcoin-miners-all-coins-mined/> accessed 17 October 2018
- Financial Action Task Force, 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' (2014) <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 3 December 2018
- Gárdos, István, 'A pénz fogalma' (2016) (1) Polgári Jog <https://gmtlegal.hu/cikkek/a-penz-fogalma.php?kid=4&did=273> accessed 11 October 2018
- Glavanits, Judit and Király, Péter Bálint, 'A blockchain-technológia alkalmazásának jogi előkérdései: a fogalmi keretek pontosításának szükségessége' (2018) (3) Jog – Állam – Politika
- Hayes, Adam, 'What factors give cryptocurrencies their value: An empirical analysis' (2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579445> accessed 13 October 2018
- Kakavand, Hossein; Kost De Sevres, Nicolette and Chilton, Bart, 'The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies' (2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251> accessed 5 November 2018
- Kerényi, Ádám and Molnár, Júlia, 'A FinTech-jelenség hatása – Radikális változás zajlik a pénzügyi szektorban?' (2017) 16 (3) Hitelintézeti Szemle
- Lo, Stephanie and Wang, J. Christina, 'Bitcoin as Money?' (2014) (4) Federal Reserve Bank of Boston Current Policy Perspective <https://www.bostonfed.org/publications/current-policy-

perspectives/2014/bitcoin-as-money.aspx> accessed 19 November 2018

- Luther, William J. and White, Lawrence H., 'Can Bitcoin Become a Major Currency?' (2014) George Mason University Working Paper in Economics, No. 14-17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446604> accessed 12 February 2019
- Madeira, Antonio, 'How legal is Bitcoin and Crypto Currencies?' (2015) <https://www.cryptocompare.com/coins/guides/how-legal-is-bitcoin-and-crypto-currencies/> accessed 23 November 2018
- Mandje, Tara, 'Bitcoin, its Legal Classification and its Regulatory Framework' (2015) 15 (2) Journal of Business & Securities Law <https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1003&context=jbsl>
- Marinoff, Nick, 'SEC Chairman: Cryptocurrencies Like Bitcoin Are Not Securities, but Most ICOs Are' (2018) <https://bitcoinmagazine.com/articles/sec-chairman-cryptocurrencies-bitcoin-are-not-securities-most-icos-are/> accessed 11 April 2019
- Mukhopadhyay, Mayukh, *Ethereum Smart Contract Development - Build Blockchain-based Decentralized Applications Using Solidity* (Pact Publishing 2018)
- Nail, Margaret, 'How infinite are cryptocurrencies?' (2017) <https://bitnewstoday.com/market/mining/how-infinite-are-cryptocurrencies/> accessed 12 February 2019
- Park, James. J., 'When Are Tokens Securities? Some Questions from the Perplexed' (2018) UCLA School of Law, Law-Econ Research Paper, No. 18-13 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298965 > accessed 16 March 2019.
- Rohr, Jonathan and Wright, Aaron, 'Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets' (2017) Cardozo Legal Studies Research Paper, No. 527 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104> accessed 21 April 2019
- Schueffel, Patrick, 'Taming the Beast: A Scientific Definition of Fintech' (2016) 4 (4) Journal of Innovation Management

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097312> accessed 4 March 2019

- Securities and Exchange Commission, 'SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities' (2017) < https://www.sec.gov/news/press-release/2017-131> accessed 19 November 2018
- Stastny, Philip 'Underpricing Effects in ICOs' (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3206323> accessed 16 March 2019
- Stylianou, Theodoros, 'An Investigation into the Utility and Potential Regulation of Initial Coin Offerings and Smart Contracts in Selected Industries and Jurisdictions' (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3276822> accessed 16 March 2019
- Tapscott, Don and Tapscott, Alex, *Blockchain Revolution: Hot the Technology Behind Bitcoin is Changing Money, Business and the World* (Portfolio Penguin 2016)
- Wurfel, Sarah, 'Blockchain is unhackable but these are 5 possible vulnerabilities of "the new Internet"' (2018) <https://captainaltcoin.com/blockchain-hacks/> accessed 13 Januar 2019
- Zetzsche, Dirk A. et al., 'The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators' (2017) University of Luxembourg Law Working Paper, No. 11/2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298> accessed 7 December 2018

Cryptocurrencies: a theoretical approach

Andrea Labancz *

Abstract: The focus of interest was relatively fast on cryptocurrencies after Satoshi Nakamoto published an online document entitled Bitcoin: A Peer-to-Peer Electronic Cash System in 2009. Even though one could face with the theoretical definition of the so-called peer-to-peer electronic cash therein, several years has passed until a legal definition related to cryptocurrencies was established by the Anti Money Laundering Directive 5 (AMLD5). In connection with the above, this study focuses on giving an introduction of the so-called cryptocurrencies from a historical point of view by highlighting the original purpose and nature of them, and by comparing cryptocurrencies with 'traditional' forms of currency among certain characteristics.

Keywords: cryptocurrency, Bitcoin, alternative virtual currency

1. Introduction

The economic crisis in 2008 has brought many changes to the financial sector.

The crisis has led to stricter rules of the financial system through the reform of the financial supervision and the lending area and the strengthening of the financial consumer protection.

The strengthening of the financial consumer protection is considered to be of paramount importance for the proper functioning of the financial system. Ensuring high level of consumer protection is necessary, given that the information asymmetry that is considered to be the fundamental feature of consumer relations plays an increased role in the financial sphere. The reason for this is the increasing complexity of the financial products.[1]

* Assistant research fellow, University of Szeged, Faculty of Law and Political Sciences, Institute of Business Law, labancz@juris.u-szeged.hu.

[1] Howells Geraint, Iain Ramsay, Thomas Wilhelmsson and David Kraft, 'Consumer law in its international dimension' in Geraint Howells, Iain Ramsay, Thomas Wilhelmsson and David Kraft (eds), *Handbook of Research on International Consumer Law* (Edward Elgar, 2010) 10-13.

In addition to the establishment of the stricter legislation, market players in the broad sense have also developed innovative, technology-based solutions. One of these is the so-called cryptocurrency.

Cryptocurrencies, due to their unclear legal status, have attracted the attention of legislators and law enforcement bodies in the short term. The difficulty of the situation regarded to cryptocurrencies is well-illustrated by the fact that while the term of ‘cryptocurrency’ is considered a common concept in the practice, the term ‘virtual currency’ or ‘crypto-asset’ is typically used by European Union’ bodies. In addition, cryptocurrencies are usually defined not only as currency or money, but also as securities, things, and property rights by theoretical studies.

AMLD5, the directive related to cryptocurrency regulation, uses and defines the term 'virtual currencies'. According to this:

> “virtual currencies means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.”[2]

[2] Council Directive 2018/843 of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing amending Directive 2015/849 and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

Concepts with similar content are used by the ECB[3], the IMF,[4] the EBA,[5] the ESMA[6] and the FATF.[7] However, according to the ENISA, cryptocurrencies are a subset of virtual currencies.[8]

It is easy to see that the issue of cryptocurrencies is closely linked to the issue of financial consumer protection. In a case, where cryptocurrencies are considered to be financial products, they fall under the scope of financial consumer protection provisions and therefore must comply with relevant legal provisions. Ensuring a high level of financial consumer protection in the EU is an area where harmonized regulation of cryptocurrencies is of paramount importance. Taking into consideration the above, the study seeks to establish a taxation of cryptocurrencies by considering a historical overview.

[3] European Central Bank, 'Virtual Currency Schemes (October 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 30 August 2019. See also ECB Crypto-Asstes Task Force, 'Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures' (May 2019) <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf> accessed 30 August 2019.

[4] Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes, 'Virtual Currencies and Beyond: Initial Considerations' (IMF Staff Discussion Note, January 2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> accessed 30 August 2019.

[5] European Banking Authority, 'EBA Opinion on 'virtual currencies' (4 July 2014) <https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 30 August 2019.

[6] European Securities and Markets Authority, European Banking Authority, European Insurance and Occupational Pensions Authority, 'ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies' (2018) <https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf> accessed 30 August 2019.

[7] Financial Action Task Force, 'FATF Report on Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 30 August 2019.

[8] European Union Agency for Cybersecurity, 'ENISA Opinion Paper on Cryptocurrencies in the EU' (September 2017) <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-opinion-paper-on-cryptocurrencies-in-the-eu> accessed 30 August 2019.

2. Brief history of cryptocurrencies

Analysing cryptocurrencies, it is necessary to consider their history. Bitcoin, the first and thus typical cryptocurrency, was established in 2009. Following its launch, a number of similar innovative financial solutions have been developed, such as Litecoin, Ether, ZCash, Monero, etc.

After the launch of Bitcoin and other cryptocurrencies, their use has begun to spread. For example, the Electronic Frontier Foundation and WikiLeaks have been accepting Bitcoin as a currency since 2011. Shortly afterwards, several market players announced the acceptance of cryptocurrencies in business transactions.[9] Cryptocurrencies are typically accepted in payment transactions as an alternative to money – essentially as an electronic exchange of digital value.

The concept of interpreting cryptocurrencies as money is confirmed by the judgment of the Eastern District of Texas of the Fifth Circuit, stating that Bitcoin is *'a currency or a form of money'*.[10] In addition, according to Germany's Finance Ministry, Bitcoin is essentially a '*unit of account*.'[11] This means that it shall be interpreted as a financial instrument. According to the Cabinet of Japan, cryptocurrencies, like Bitcoin, have a function similar to money; and adopted legislation in 2017 to make Bitcoin transactions *de iure* payment transaction.[12]

In general, it can be stated that the closer in time the innovative solutions called cryptocurrencies are to Bitcoin, the more likely they have similar features to it; so that they can serve as a basis for research. However, as time passes, it is likely that innovative financial solutions can be used for different purposes as Bitcoin; consequently, they may not necessarily be interpreted as cryptocurrency. Characteristics such as being an alternative to traditional payment, existing in a peer-to-peer system and being decentralized, using specific IT procedures, using

[9] As for examples WordPress, the Internet Archive, University of Nicosia, the Overstock.com, Newegg, Dell, Microsoft, Steam, and different businesses.

[10] Securities and Exchange Commission v. Shavers et al, No. 4:13-CV-416 (E.D. Tex. 2013).

[11] Luong Hoang Anh, 'The Story of Bitcoin Part 1' (*Medium*, 26 July 2018) <https://medium.com/twogap/the-story-of-bitcoin-449de3c49493> accessed 30 August 2019

[12] Garrett Keirns, 'Japan's Bitcoin Law Goes Into Effect Tomorrow' (*CoinDesk*, 31 March 2017) <https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow> accessed 30 August 2019

mining as a key element and being convertible should be considered specific features in case of cryptocurrencies.[13]

Given the above, when establishing the taxation, cryptocurrencies need to be compared primarily with the legally relevant topics of 'money' and further examined under this factor. To do this, it is first necessary to define the legally relevant concept of money.

3. Formation and regulation of 'money'

In the taxonomy of cryptocurrencies, the examination of historical factors plays a prominent role. In this context, it is first necessary to examine the establishment and development of money.

In this context, it should be noted that there is a strong correlation between the development of money and the development of commerce; money should be considered the result of simplifying commercial relations, as follows.

The period of 'barter' should be considered the first stage in the development process, where commodities were acting as money. The value of commodities was determined by the value of other commodities and the exchange of goods based on consensus. However, the process was made difficult since determining the relative value of the goods was concerned.[14]

The issue was solved in the period of 'commodity money', where generally accepted exchange tools were used as money. Such means of exchange were also goods; those which, by virtue of their specific characteristics, were suitable for use as commodities (value stability, divisibility, uniformity, transportability, general acceptance).[15] Examples

[13] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) <https://bitcoin.org/bitcoin.pdf> accessed 30 August 2019; 'Lite Coin White Paper' <http://zioncoins.co.uk/wp-content/uploads/2015/06/Lite-Coin-Whitepaper.pdf> accessed 30 August 2019; Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer and Madars Virza, 'Zerocash: Decentralized Anonymous Payments from Bitcoin' (18 May 2014) <http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf> accessed 30 August 2019; 'A Next-Generation Smart Contract and Decentralized Application Platform' <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 30 August 2019.

[14] Jaksity, György, *A pénz könnyelmű természete* (Alinea Kiadó 2005) 29-30.

[15] Gárdos, István, 'A pénz fogalma' (Gárdos, Mosonyi, Somogyi Ügyvédi Iroda, 6 March 2016) <

include salt, cattle or shell, etc. During this period, it was also necessary for commodities to have an intrinsic value, which contributed to the development of social trust towards them.[16]

During the Bronze Age, the use of precious metals served as a medium of exchange, where coins were used as money. However, given the limited availability of precious metals, other means of exchange were needed.[17]

The change was linked to early technological development. In the period of the Industrial Revolution, due to economic development and mass production, merchants began to issue bills of exchange as promises of payment. The development of banknotes should be considered the next step in the process, which resulted in banks issuing a bill of exchange on their own behalf, committing themselves to paying upon presentation. It was another dimension when the state entered into the process and already had the sole right to issue banknotes to unify the country's currency.[18]

The development of technology has led to the appearance of account money; and the development of e-commerce has led to the creation of e-money.[19]

Obviously, with the development of money, the need for regulation has occurred. An important part of the provisions relating to money should be considered under the topic of payment services. In this context, it should be examined whether cryptocurrencies fall under the scope of the regulated categories of money. To do this, the specifics of the parties and the subject of the transaction, the issuance and the convertibility need to be discussed under the topic of financial characteristics.

Institutional players of traditional payment transactions should be considered the parties of the transaction, so that central banks and financial institutions.

In the two-level bank system, the central bank only indirectly contacts customers, through financial institutions. The tasks of the central bank include monetary policy, banknote and coin issuance, the management

https://gmtlegal.hu/upload/G__rdos_Istv__n_A_p__nz_fogalma_Polg__ri_Jog.pdf> accessed 30 August 2019.

[16] Gárdos (n 15)

[17] Jaksity (n 14) 30-38

[18] ibid 41, see also Gárdos (n 15)

[19] Fehérvári Erzsébet, *Online banking, Elektronikus banki szolgáltatások* (AKAPRINT 2008) 13-15.

of the country's foreign exchange and gold reserves, ensuring the smooth flow of payments and supporting the stability of the financial system.[20]

There are two sub-categories of financial institutions: credit institutions and financial enterprises. These institutions must meet strict statutory requirements related to the establishment and operation.[21] Only these institutions, subject to certain exceptions, can professionally provide financial services by having a license. Such activities include, but are not limited to, providing payment services or issuing of electronic money.[22]

Apart from financial institutions, payment institutions should also be considered which are engaged in activities related to payment services. Similarly to financial institutions, these institutions must meet statutory requirements related to their establishment and operation. The rules cover the licensing, the amount of the solvency margin and initial capital, the protection of client funds, the scope of the activities, liability and supervision.[23]

With the development of e-commerce, electronic money institutions have also been established, and later regulated. Strict requirements related to the commencement, continuation and prudential supervision of electronic money institutions have also been developed.[24]

[20] Ernő Huszti, Pál Péter Kolozsi and Csaba Lentner, 'Jegybanki szabályozás és monetáris politika Magyarországon' in Lentner, Csaba (ed), *Bankmenedzsment* (Nemzeti Közszolgálati és Tankönyv Kiadó 2012) 112-124.; see also László Bódy, Katalin Botos, Klára Schneider, József Zavodnyik, József Rotyis and Andás Nemescsói, *Magyar pénz- és tőkepiaci rendszer* (Osiris 2001) 16-22.

[21] Council Directive 2013/36/EU of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC [2013] OJ L176/338, Council Regulation 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 [2013] OJ L176/1.

[22] Bálint Csere and Márta Quirin, 'Hitelintézetek és pénzügyi szolgáltatást végző egyéb szervezetek jogi szabályozása' in Lentner Csaba (ed), *Bankmenedzsment* (Nemzeti Közszolgálati és Tankönyv Kiadó 2012) 209-217.

[23] Council Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35.

[24] Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending

The direct object of the transaction is the payment transaction, the indirect object is the money itself. Payment transaction shall mean any payment, transfer or withdrawal of funds by or on behalf of the payer, irrespective of the underlying obligations between the payer and the payee.[25]

Money is at the heart of these payment transactions. It should be noted that legislation defines money-related terms with different content. The category of legal tender includes banknotes and coins issued in an official currency of a country; the category of payment services includes banknotes, coins, account money, and electronic money;[26] the category of payment instrument includes a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order.[27]

Consequently, a distinction may be made between the material and the non-material appearance of money. Banknote and coin should be considered under the category of material appearance of money, while account money and electronic money should be considered under the category of non-material appearance of money.[28] While banknotes and coins may circulate as cash; account money, in an IT sense, is an electronic sign stored in a financial institution, and, in a legal sense, a deposit account held in a credit institution or central bank account and essentially means a deposit on a payment account of indefinite

Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7.

[25] Council Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35.

[26] Council Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35.

[27] Council Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35.

[28] Ziád Bánfi, 'A Bitcoinról pénzelméleti szempontból' (2018) 1 (5) Gazdaság és Pénzügy <http://www.bankszovetseg.hu/Public/gep/2018/002-30ig%20Banfi%20Ziad.pdf> accessed 30 August 2019.

duration;[29] and electronic money is a monetary value, represented by a claim on the issuer, stored electronically, including magnetic storage, issued on receipt of funds for the purpose of making payment transactions and accepted by any person other than the issuer. Such payment transaction shall be any payment, transfer or withdrawal of funds by or on behalf of the payer, irrespective of the underlying obligations between the payer and the payee. [30] Electronic money may be stored electronically, for example, on mobile phones or online payment accounts.

Given that both account money and electronic money are based on technological solutions, their safe technological operation is standardized. In case of using account money via a payment instrument, it is needed to comply with the Europay–MasterCard–Visa (EMV standard) standards for international payment cards. The EMV standard has been developed to make payment card transactions more secure and to increase confidence in payment cards.[31] Similarly to account money, in case of electronic money, standardized solutions play an important role, so that the CEPS (Common Electronic Purse Specifications) should be considered.

It is also necessary to refer to the issuance of money. The exclusive right of issuing legal tender is typically linked to a central body, more specifically to the central bank, which is responsible for the circulation of banknotes and coins.[32] Commercial banks and the central bank are authorized to create account money, and legal persons, by having a license, may issue electronic money.[33] It should be noted that in all three cases (cash, account money, electronic money), a body or an enterprise is authorized to issue money by having license. Essentially, this should be

[29] Gárdos (n 15).

[30] Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7. See also Bánfi (n 28).

[31] Central Bank of Hungary, 'Pénzforgalomról mindenkinek 1.' (2008) <https://www.mnb.hu/letoltes/penzforgalomrol-mindenkinek-bankkartyak.pdf> accessed 30 August 2019

[32] Bódy, Botos et al. (n 20) 17-18.

[33] Council Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7, Art 2 point 1.

considered a kind of a centralized characteristic in the process of issuing money.

Today's money is typically convertible, meaning that one nation's currency (foreign currency) is typically convertible to another nation's currency. It should be noted that in international commerce and, increasingly in e-commerce, it is of utmost importance that each service be defined in the legal tender of a nation.

Summarizing the above, it should be highlighted that the characteristic of being accepted by persons other than its issuer should be considered the general feature of money. The development of money cannot be considered closed; money is undergoing constant changes as a result of socio-economic and technological developments. In this context, persons and bodies issuing the money, commodities accepted as money and the form of money should be considered. At the same time, the ideology of the cashless economy is becoming more and more widespread. In addition, trust should be considered an important social factor relevant to the development of money, which is intended to be guaranteed by law through consumer protection provisions.[34]

4. Cryptocurrencies in light of money regulation

As defined above, trust should be considered the basis of traditional payment transactions. Similarly, cryptocurrencies are also built on trust. The Bitcoin system has a closely tight link to the financial crisis in 2008. Essentially, it has evolved from it to address the financial and confidence issues arisen from the crisis.

An Edelman's survey from 2019 entitled Trust Barometer examined trust and credibility of people in institutions and organizations. According to the survey, the level of trust in institutions has declined significantly over the last 10 years, while the level of trust in self-managed relationships is increasing. According to the survey, the technology sector is leading the confidence index in each industry, while the financial sector is the least trusted, but with the highest confidence growth.[35]

[34] Bánfi (n 28).

[35] 'Trust Barometer' (*Edelman*, 2019) <https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Global_Report_0.pdf?utm_source=website&utm_medium=global_report&utm_campaign=downloads> accessed 30 August 2019.

The results of the survey can be compared with the increasing use of cryptocurrencies. According to Satoshi Nakamoto's work, the basic purpose of creating Bitcoin is to exclude financial institutions as trusted third parties from participating in payment services.[36] This parallel leads to an alternative to the two-level bank system by establishing a special payment and settlement system for cryptocurrencies, called the blockchain.

In terms of financial characteristics, the parties of cryptocurrency transactions are therefore not financial institutions, payment institutions or electronic money institutions. Legally relevant features of such a peer-to-peer system include the ability to execute payment transactions without the involvement of financial intermediaries and the ability to execute each payment through an electronic communications network.

One particular difference is the anonymity of the account holders and the transparency of the transactions.[37]

Transactions should be considered *quasi* payment services or transactions, which focused on cryptocurrencies. In their form, cryptocurrencies are similar to account money and electronic money since payments appear as data (digital signals) and cryptocurrencies appear as a series of digital signatures. All this means that cryptocurrencies have non-material form. The parties and the subject of the transactions are linked in such a way that the beneficiary of the *quasi* payment transactions also strengthens the chain of former owners by confirming the digital signature.[38]

Despite similarities, there are important differences between traditional forms of money and cryptocurrencies. These differences are most likely to be interpreted in light of the centralized-decentralized binary code analysis.

While traditional payment transactions are established and executed typically in a centralized model, cryptocurrency transactions are established and executed in a decentralized model. The decentralized model is characterized by the fact that not only a special institution has decision-making autonomy but many local players, as nodes. This also

[36] Nakamoto (n 13).

[37] Eszteri Dániel, 'Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze?' [2012] Infokommunikáció és Jog 71.

[38] Bánfi (n 28).

means that while the information distribution of the centralized system is vertical, the information distribution of the decentralized system is horizontal between nodes.[39]

Examining the decentralized model in case of cryptocurrencies, both at the moment of 'issuance' and the execution of each transaction should be considered of significant importance. Although we cannot talk about issuing money in the traditional sense, a specific issuing method may be examined. Mining may be defined as an alternative to issuing new cryptocurrency, since miners are using software to help creating new cryptocurrencies and get them into the system by solving mathematical problems.[40] Consequently, the community of mining can be interpreted as a *special or quasi issuer*.

Distributed feature of cryptocurrencies (which can occur in both centralized and decentralized systems) should also be considered. The distributed system means that there are different nodes in the system that communicate continuously with each other. However, the distributed character does not equal with the decentralized character; a centralized system can be distributed. In a distributed and decentralized system, nodes are interconnected.[41]

It is also necessary to identify specific IT procedures. These include the hash function, the digital signature and cryptography that is able to distinguish cryptocurrencies from other forms of money.[42]

5. A possible taxonomy

Given the many specific features of cryptocurrencies, it should be emphasized that, inter alia, they shall be interpreted under the category of the legally relevant money if they existed in connection with a pecuniary claim against a financial institution, or could be used to access cash in

[39] Kirankalyan Kulkarni, *Learn Bitcoin and Blockchain* (Packt, 2018) ch 3

[40] Cf. Marcell Tüzes, 'Bitcoin – A pénz új formája' [2012] Infokommunikáció és Jog 155.

[41] Kulkarni (n 39).

[42] See János Folláth, Andrea Huszti, Attila Pethő, *Informatikai biztonság és kriptográfia* (Kempelen Farkas Hallgatói Információs Központ, 2011).

charge of pecuniary claim or could be used as remuneration of transactions. In view of the above, this is conceptually excluded.[43]

Examination of cryptocurrencies concluded that they could not be interpreted under the current and legally relevant concept of money. However, it is not a negligible circumstance that they typically perform almost all the economic functions of money.[44] Therefore, it seems logical to take the view, on the one hand, that cryptocurrencies are similar in purpose and nature to money, and, on the other hand and on the basis of the first observation, could be defined as another dimension of the development of money.

It is also appropriate to agree with the view that any commodity can function as money, given that money is mostly a symbol system.[45]

Therefore, in order to address the legal uncertainty surrounding cryptocurrencies, a possible taxonomy needs to be established.

In such a taxonomy, payment instruments may be the broadest category. This category should be interpreted as a broadly defined set in which both traditional and innovative payment instruments can be placed. Within the category of payment instruments, the regulated payment instruments can take place. These are banknotes, coins, account money and electronic money, so that the material and non-material forms of money.

Payment instruments intended to provide an alternative to traditional money, differ from the category of regulated payment instruments. Given that these alternative solutions typically mean virtual solutions, it is advisable to refer to these devices as alternative virtual payment instruments. Essentially, the category of alternative virtual payment instruments should be considered approximately equal with the category of the European Union' definition of virtual currency. A common feature of the category of alternative virtual payment instruments is that they originate from intense innovation efforts of the 21st century. In this category cryptocurrencies can be interpreted as a subset because of their

[43] Hungarian Financial Supervisory Authority, 'Papíralapú ajándékutalvány készpénz-helyettesítő fizetési eszköznek minősül-e?' <http://alk.mnb.hu/data/cms2103337/penz17.pdf> accessed 30 August 2019.

[44] See Tamás Gábor and Gábor Dávid Kiss, 'Bevezetés a kriptovaluták világába' (2018) 1 (5) Gazdaság és Pénzügy <http://www.bankszovetseg.hu/Public/gep/2018/002-30ig%20Banfi%20Ziad.pdf> accessed 30 August 2019.

[45] Bánfi (n 28).

above-defined distinctive features. Taking into consideration these features, the study considers the concept of cryptocurrency developed by the ENISA to be acceptable, according to which

> "cryptocurrency refers to a math-based, decentralized convertible virtual currency that is protected by cryptography. - i.e., it incorporates the principles of cryptography to implement a distributed, decentralized, secure information economy."[46]

Within the category of alternative virtual payment instruments, virtual payment instruments do not meet the criteria of cryptocurrencies may mean a further subcategory.[47] Centralized, non-convertible, non-mineable virtual payment instruments are not considered *de facto* cryptocurrency under this study. Given that these are typically FinTech solutions, it may be advisable to define them as FinTech virtual currencies.

Although not of particular relevance for the purposes of the study, it is necessary to refer to a third sub-category. This is the category of personal data which can also be used as payment instrument in the 21st century.

It is necessary to distinguish instruments can only be validated on a limited network from the category of alternative virtual payment instruments. All this means that these instruments cannot leave the network in which they represent value. More precisely, they represent value only in the network and for the parties of the network. Subcategories can also be created in this category. Such a subcategory may include virtual payment instruments that can only be used in computer games. Alternatively, another sub-category may be set up by different cards and value stored on them issued by businesses.

6. Summary

The aim of the study is to examine cryptocurrencies. In connection with cryptocurrencies, it is necessary to emphasize that the general trust

[46] European Union Agency for Cybersecurity (n 8).
[47] As for examples centralized Ripple or LibraCoin (Facebook).

should be considered the basis of the functioning of the monetary system. The role of trust, though a sub-legal factor, is unquestionable in the financial sector. For an instrument to be universally accepted as money, it is necessary to build social trust in it. This social trust naturally develops and consolidates if the instrument itself is reinforced by a system of state guarantees. These guarantees may be summed up in the provisions of consumer protection law and in the financial sphere, in the provisions of financial consumer protection law.[48]

However, in the age of digitalization, the question arises whether the role of a guarantee system can still be fulfilled only by the state or an IT system that is transparent, robust and secure due to the use of technological solutions can also meet the said criteria.

In order to answer the question, a test was carried out in which the parties, the subject, the financial and IT features of the transaction were emphasized. As a result of the test, it can be concluded that cryptocurrencies do not fall into the legally relevant category of money, and therefore cannot be subject to financial consumer protection provisions. In addition to the establishment of taxonomic categories, regarding the financial consumer protection needs expressed above, the question of possible regulation arises. Beside this, it is necessary to take into account the enhanced technological nature of the area. Strict legal provisions do not necessarily mean the best solution for regulating technology. Instead, technology solutions are typically standardized.

In addition, it is necessary to point out the fact that, in the field of cryptocurrencies, the technological and IT characteristics ensure that the system operates almost without error and misuse. These characteristics may be suitable for meeting the requirement of high confidence in the financial sector.

Ensuring the possibility of self- and co-regulation for alternative payment instruments may be an open question for the future regulation. It is easy to see that cryptocurrencies relate to traditional money as self- and co-regulation relate to traditional law: they are an alternative.

[48] See Council Directive 2014/49/EU of 16 April 2014 on deposit guarantee schemes [2014] OJ L173/149, Council Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35, Council Directive 2014/65/EUof 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349 or the FIN-NET.

References

- 'A Next-Generation Smart Contract and Decentralized Application Platform' <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 30 August 2019
- Bánfi Z., 'A Bitcoinról pénzelméleti szempontból' (2018) 1 (5) Gazdaság és Pénzügy <http://www.bankszovetseg.hu/Public/gep/2018/002-30ig%20Banfi%20Ziad.pdf> accessed 30 August 2019
- Ben-Sasson E., Chiesa A., Garman C., Green M., Miers I., Tromer E. and Virza M., 'Zerocash: Decentralized Anonymous Payments from Bitcoin' (18 May 2014) <http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf> accessed 30 August 2019
- Bódy L., Botos K., Schneider K., Zavodnyik J., Rotyis J. and Nemescsói A., *Magyar pénz- és tőkepiaci rendszer* (Osiris 2001)
- Central Bank of Hungary, 'Pénzforgalomról mindenkinek 1.' (2008) <https://www.mnb.hu/letoltes/penzforgalomrol-mindenkinek-bankkartyak.pdf> accessed 30 August 2019
- Csere B. and Quirin M., 'Hitelintézetek és pénzügyi szolgáltatást végző egyéb szervezetek jogi szabályozása', in Lentner Cs. (ed), *Bankmenedzsment* (Nemzeti Közszolgálati és Tankönyv Kiadó 2012)
- ECB Crypto-Asstes Task Force, 'Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures' (May 2019) <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf> accessed 30 August 2019
- Edelman, 'Trust Barometer' (2019) <https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Global_Report_0.pdf?utm_source=website&utm_medium=global_report&utm_campaign=downloads> accessed 30 August 2019
- European Banking Authority, 'EBA Opinion on 'virtual currencies'' (4 July 2014) <https://eba.europa.eu/documents/10180/657547/EBA-Op-

2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 30 August 2019

- European Central Bank, 'Virtual Currency Schemes' (October 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 30 August 2019
- Eszteri D., 'Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze?' [2012] Infokommunikáció és jog 71
- European Securities and Markets Authority, European Banking Authority, European Insurance and Occupational Pensions Authority, 'ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies' (2018) <https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf> accessed 30 August 2019
- European Union Agency for Cybersecurity, 'ENISA Opinion Paper on Cryptocurrencies in the EU' (September 2017) <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-opinion-paper-on-cryptocurrencies-in-the-eu> accessed 30 August 2019
- Fehérvári E., *Online banking, Elektronikus banki szolgáltatások* (AKAPRINT 2008)
- Financial Action Task Force, 'FATF Report on Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (June 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 30 August 2019
- Folláth J., Huszti A. and Pethő A., *Informatikai biztonság és kriptográfia* (Kempelen Farkas Hallgatói Információs Központ 2011)
- Gábor T. and Kiss G., 'Bevezetés a kriptovaluták világába' (2018) 1 (5) Gazdaság és Pénzügy <http://www.bankszovetseg.hu/Public/gep/2018/002-30ig%20Banfi%20Ziad.pdf> accessed 30 August 2019
- Gárdos I., 'A pénz fogalma' (Gárdos, Mosonyi, Somogyi Ügyvédi Iroda, 6 March 2016) <https://gmtlegal.hu/upload/G__rdos_Istv__n_A_p__nz_fogalma_Polg__ri_Jog.pdf> accessed 30 August 2019

- He D., Habermeier K., Leckow R., Haksar V., Almeida Y., Kashima M., Kyriakos-Saad N., Oura H., Saadi Sedik T., Stetsenko N. and Verdugo-Yepes C., 'Virtual Currencies and Beyond: Initial Considerations' (IMF Staff Discussion Note, January 2016) <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf > accessed 30 August 2019
- Hoang Anh L., 'The Story of Bitcoin Part 1' (*Medium*, 26 July 2018) <https://medium.com/twogap/the-story-of-bitcoin-449de3c49493> accessed 30 August 2019
- Howells G., Ramsay I., Wilhelmsson T. and Kraft D., 'Consumer law in its international dimension' in Howells G, Ramsay I, Wilhelmsson T and Kraft D (eds), *Handbook of Research on International Consumer Law* (Edward Elgar 2010)
- Hungarian Financial Supervisory Authority, 'Papíralapú ajándékutalvány készpénz-helyettesítő fizetési eszköznek minősül-e?' <http://alk.mnb.hu/data/cms2103337/penz17.pdf> accessed 30 August 2019
- Huszti E, Kolozsi P and Lentner Cs, 'Jegybanki szabályozás és monetáris politika Magyarországon' in Lentner Csaba (eds), *Bankmenedzsment* (Budapest 2012)
- Jaksity Gy., *A pénz könnyelmű természete* (Alinea Kiadó 2005)
- Keirns G., 'Japan's Bitcoin Law Goes Into Effect Tomorrow' (*CoinDesk*, 31 March 2017) <https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow> accessed 30 August 2019
- 'Lite Coin White Paper' <http://zioncoins.co.uk/wp-content/uploads/2015/06/Lite-Coin-Whitepaper.pdf> accessed 30 August 2019
- Nakamoto, S., 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) <https://bitcoin.org/bitcoin.pdf> accessed 30 August 2019
- Securities and Exchange Commission v. Shavers et al, No. 4:13-CV-416 (E.D. Tex. 2013)
- Tüzes M, 'Bitcoin – A pénz új formája' [2012] Infokommunikáció és Jog 155
- World Bank Group, 'Distributed Ledger Technology (DLT) and Blockchain' 2017) <http://documents.worldbank.org/curated/en/1779115137140

62215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 30 August 2019

Short biography of the author

Dr. Andrea Labancz works at the Institute of Business Law of the Faculty of Law and Political Sciences of the University of Szeged as an assistant research fellow since September 2018 where she teaches business related issues. Since 2017, she is a PhD student of the Doctoral School of the Faculty of Law and Political Sciences of the University of Szeged. Her research area includes consumer protection law, especially in the area of financial innovation.

III. Business and digitalization

Adoption of ICT in Higher education: Readiness of University Students in Rural India

Neera Chopra*

Abstract: Rapid advancement in Information and Communication Technology over the past two decades has affected human life in every respect; education sector being no exception. World over, Higher Education Institutions (HEIs) have adopted ICT for enhancing their efficiency and effectiveness. India has undertaken a number of policy initiatives to promote the use of ICT in HEIs in the country. Available secondary data clearly shows that the penetration of Internet into rural India is only a fraction of the figure for urban India. In light of the above, this paper will find answers to the following questions: 1) What is the current level and preparedness of students regarding adoption of ICT in Universities located in rural India 2) What are the technology needs and preferences of these students for Academic purposes and what is the readiness of the system to fulfil those?

The study uses the DigComp framework developed by the European Commission that examines digital competence on the parameters of internet safety awareness, digital communication, creating digital content and problem solving. Primary data is collected using structured questionnaire, with close-ended questions, from 260 students in four pre-selected universities from rural India. The study will be divided into two parts: 1) discussion on the Higher Education system in rural India and the role of ICT through a review of the relevant literature, leading up to the formulation of the objectives of the research 2) detailed analysis of the findings to answer the research questions.

Keywords: India, HEIs, ICT, Digital competence, rural students

1. Introduction

Rapid advancement in Information and Communication Technology over the past two decades has affected human life in every respect; education sector being no exception. The landscape of teaching and learning is changing with digital technologies like internet, computers and mobiles accelerating student's learning, enhancing access to educational

* PhD student, National University of Public Service, Doctoral School of Public Service Sciences (Budapest).

opportunities, and supporting interactivity, interaction and collaboration.[1] The advantages of digital technologies are ubiquitous because of the unique features of technologies, which include portability, low cost, personalization and improved communication abilities and interactivity. World over, Higher Education Institutions (HEIs) are investing in ICTs for enhancing their efficiency and effectiveness not just in the administrative management but also in academic management. In both developed and developing countries digital technologies have become an icon of 21st century higher education provision. In this changing educational landscape, learners require new literacies. In recent years, digital competence has become a key concept in discussions on the kind of skills and understanding learners need in the Knowledge Society.[2]

India has a population of 1.35 billion and a high population among them is young and enrolled in higher education. According to 2011 census, 72% of the population resides in rural areas and 28% live in urban conglomerates. The ICT infrastructure in rural areas is limited and not evenly distributed. On the other hand the urban areas have the right infrastructure and high internet penetration. The studies show that there is an urban rural divide and two thirds of the population in India do not have access to internet.[3] The review of literature suggests that socio-economic barriers like poverty, illiteracy, poor awareness of technology has restrained the growth of digital literacy in rural India. This divide is prevalent in urban–rural education institutions also. HEIs located in urban areas have better access to new technologies compared to the institutions located in rural or semi-urban areas. Hence urban academic institutions can equip students with better knowledge of ICT.

In the last decade, however, India has escalated its efforts to bridge the rural urban digital divide in terms of infrastructure and internet penetration. India has taken giant leaps in recent years to use ICT in its education system. The Government of India came up with the idea of

[1] N. Selwyn, 'The use of computer technology in university teaching and learning: a critical perspective' 2007 23 (2) Journal of Computer Assisted Learning (doi:10.1111/j.1365-2729.2006.002) 83–94.

[2] Eliana Gallardo-Echenique, Janaina Minelli de Oliveira, Luis Marqués-Molias and Francesc Esteve-Mon, 'Digital Competence in the Knowledge Society' (2015) 11 MERLOT Journal of Online Learning and Teaching 1-16.

[3] Amit Singh Khokhar, 'Digital Literacy: How Prepared Is India to Embrace It?' 2016 7 (3) International Journal of Digital Literacy and Digital Competence 1-12.

promontory use of ICTs in education in its Twelfth Five-Year Plan (2012-2017). There are plenty of ICT projects launched in India, which help and motivate learners to learn using ICT tools. A study by Sampath states that initiatives have been taken to implement ICT-integrated education and enabling provision of ICT-integrated examination and e-governance at the institutional and systemic level including setting up of education portal(s) (India Planning Commission, 2013).[4] E-Gyankosh, which aims at preserving digital learning resources is a knowledge repository launched by IGNOU, the National Open University. Almost 95% of IGNOU's printed material has been digitized and uploaded on the repository. The National Programme for Technology Enhanced Learning (NPTEL) launched in 2001 is another joint initiative of IITs and IISc which promotes education through technology. The National Mission on Education through ICT is centrally sponsored scheme submitted by the Ministry of HRD (Human Resource Development) and approved by the Cabinet Committee on Economic Affairs (CCEA). The Mission has planned a variety of initiatives aimed at developing and standardizing digital content for Indian higher education segment. The Mission envisions catering to the learning needs of 500 million people in the country.[5]

But all these initiatives can be fully successful only if these digital resources are accessed and adopted by students of rural India; at the same time penetration of appropriate infrastructure needed for digital access should also be available in rural India. We are yet to achieve the desired level of ICT adoption in higher education in the whole country. One of the reasons for the underutilisation of these initiatives is the low level of digital literacy among the rural students. The majority of Indians living in rural areas have poor access to internet, it is necessary that they are exposed and trained in basic computing skills and ICT utilization. Extending and improving digital competence is an essential component in the development of employable graduates. Since 90% of new jobs will

[4] B.T. Sampath Kumar and S.U. Shiva Kumara, ' The digital divide in India: use and non-use of ICT by rural and urban students' 2018 World Journal of Science, Technology and Sustainable Development <https://www.emerald.com/insight/content/doi/10.1108/WJSTSD-07-2017-0021/full/html?fullSc=1&mbSc=1>.

[5] U. K. Pegu, 'Information and Communication Technology in Higher Education in India: Challenges and Opportunities' (2014) 4 International Journal of Information and Computation Technology 513-518.

require excellent digital skills, those without sufficient ICT skills will be at a disadvantage in the labour market and have less access to information. Digital literacy enables us to match the medium to the information presented and to the audience targeted.[6] ICT can be effectively used to enhance the quality of learning and create social payoffs, which would be conducive to sustainable growth and equitable development.[7]

With this background, the study has been conducted to assess the digital competence of rural students in Higher Education on their Readiness i.e. the ability to understand and appreciate digital technology. This study will help HEIs design the innovative use of ICT based on the students' needs and abilities in the rural areas aimed at embedding digital competences into curriculum development and delivery.

2. Digital Competence

In the 1990s computers were limited in availability to a few professionals, but with advances in technology there has been a shift from programming languages to graphic user interfaces, the technologies have become user friendly and more available to the society.[8] Now there is a need to take advantage of technology and to be functional in society, digital competence or literacy is the essential requirement of life. Today it is paramount that every citizen should have the opportunity to experience the value, technology can bring into the way they live, work and exist. Digital Literacy is recognised as one of the UN's Sustainable Development goals. It has also been officially recognised that digital literacy is of the same importance as reading, writing and numeracy.[9] According to OECD,[10] Digital competence has both become a requirement and a right. India has also recognised that building digital skills is as essential as creating digital infrastructure. Apart from providing the infrastructure, government has

[6] C. Lankshear and M. Knobel, *Digital Literacies – Concepts, Policies and Practices* (Peter Lang 2008).

[7] A. M. Barret, 'The Education Millennium Development Goals Beyond 2015: Prospects for Quality and Learners, EdQual Working Paper No. 13, 2009.

[8] Expert views on DIGCOMP, see A. Ferrari, 'Digital Competence in Practice: An Analysis of Frameworks' (2012) European Commission JRC 68116.

[9] Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning. OJ L 394, 30.12.2006, 10–18.

[10] OECD, *PISA 2009 Results: What Students Know and Can Do. Students performance in reading, mathematics and science* (vol. 1, OECD 2010)

also launched National Digital Literacy Mission to impart training to one person in every family where none of the members are digitally literate so as to enable them to take part in citizenship through e-governance. But what exactly is meant by digital skills?

It has been interpreted in various ways (e.g. Digital Literacy, Digital Competence, e Literacy, e-Skills, e Competence, Computer literacy, and Media literacy) in policy documents, in the academic literature, in teaching, learning and certification practices. All these terms highlight the need to handle technology in the digital age.[11] So we understand that the concept of digital Competence is a multi-faceted moving target, covering many areas and literacies and rapidly evolving as new technologies appear. According to Ferrari, being digitally competent today implies the ability to understand media, to search for information, be critical about what is retrieved and be able to communicate with others using variety of digital tools and applications. Further, the concept is much wider than the ability to use a specific set of tools or applications. Digital competence is not centred on a tool oriented perspective only.[12] Eshet argued that digital literacy is more than just using software as it covers most of the cognitive skills like reading instructions, using digital reproduction in learning and, evaluating information.[13] The study provided a holistic conceptual model to effectively utilise digital literacy in educational contexts. Alkali and Hamburger built upon the work of Eshet (2002) by arguing that digital literacy comprises of five digital skills namely: photo-visual skills, reproduction skills, branching skills, information skills and, socio-emotional skills.[14] An institutional definition comes from the European Commission. Digital competence, as defined in the European Parliament and the Recommendation on Key Competences for Lifelong Learning of the Council of the European Union,[15] 'involves the confident and critical use of Information Society Technology (IST) for work, leisure and communication. It is underpinned by basic skills in ICT: the use of computers to retrieve, assess, store, produce, present and exchange

[11] Ferrari (n 8).

[12] Y. Eshet, 'Digital literacy: A new terminology framework and its application to the design of meaningful technology-based learning environments' (2002) ERIC Paper 143.

[13] Eshet (n 12) quoted by Khokhar (n 3).

[14] Y. E. Alkali and Y. Amichai-Hamburger, 'Experiments in digital literacy' 2004 7 (4) CyberPsychology & Behavior (doi:10.1089/cpb.2004.7.421 PMID:15331029) 421–429, quoted by Khokhar (n 3).

[15] Recommendation (n 9) 13.

information, and to communicate and participate in collaborative networks via the Internet'.

We can see that the scope of digital skills has changed over the years. After a focus on access of ICT and Internet in the 1990s, a new type of digital divide has appeared which goes beyond access. As society is becoming digitised, the knowledge, skills and attitudes that are needed are becoming manifold: being digitally literate today is not restrained to the understanding of hardware and software devices. It now encompasses the knowledge, skills and attitude needed to be digitally competent. The management of information and ability to use the internet with the knowledge about the risks of internet are seen as crucial fields. Moreover critical thinking, creativity and innovation are essential aspects of digital competence.[16] The all-encompassing definition of Digital Competence thus is:

Digital Competence is a set of knowledge, skills, attitudes (thus including abilities, strategies, values and awareness) that are required when using ICT and digital media to perform tasks; solve problems; communicate; manage information; collaborate; create and share content; build knowledge efficiently; appropriately, critically, autonomously, flexibly for work, leisure, participation, learning, socialising, consuming and empowerment.[17]

We now come to understand that the ability to use specific tools and applications is just one of the several competence areas that need to be developed by citizens in order to function in a digital environment. The concept of digital competence includes domains such as internet safety awareness, digital communication, creating digital content and problem-solving. This understanding of digital competence is in line with the digital competence framework initiated by the European Commission.[18] The other areas that need to be taken into account for a multi-dimensional approach and more adapted to the current needs is as per the framework developed by Digcomp.

[16] Ferrari (n 8).
[17] ibid.
[18] ibid.

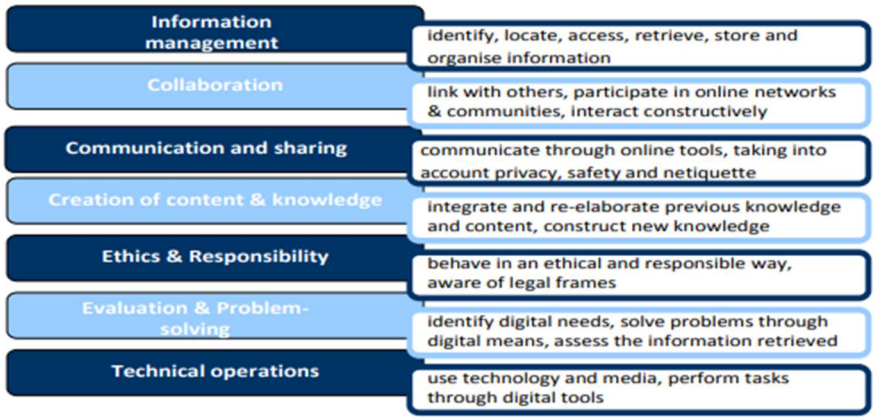


Figure 1: The Digcomp framework (source: Ferrari 2012)

World over, new digital readiness programmes are being set by the respective governments to coordinate initiatives on digital inclusion, cyber safety, information and media. Policy makers and educational institutions need to be at the forefront to devote resources to educate citizens and future citizens to become digitally competent and become functional in this digitised world.

As mentioned earlier, 72% of India's population lives in rural areas, while 28% lives in towns and in urban conglomerates. Poor access to technology, besides poverty, illiteracy and a general lack of awareness has restrained the growth of digital literacy in rural India. It is rather disappointing that while in the developed world the divide is over skills and attitude, in India the argument of digital divide persists. There is no dearth of initiatives in the form of schemes and resources earmarked by the Government of India to bridge this divide, more so in the field of Higher Education as discussed in the preceding sections. This study aims to examine the digital competence among students of Higher Educational Institutes in rural India. The following section discusses the objectives of the study in detail.

3. Objectives of the study

The literature on ICT penetration in India suggests an urban rural divide. The perception is that socio-economic barriers like poverty, illiteracy, poor awareness of technology has restrained the growth of digital literacy in rural India. Affordability of digital technology is a major challenge in rural India with low average incomes. India's linguistic diversity and limited penetration of English language creates availability gridlock. Concurrently, Government of India has introduced many digital initiatives in Higher Education to educate the masses, thus breaking the barrier of cost and entry, especially to vulnerable groups, using the latest technology available. MOOCs developed by qualified and exceptional teachers on the SWAYAM platform is such an example in India. The study by Sampath shows that the Massive Open Online Courses (MOOCs) have emerged as one of the most promising methods of catering higher education in an open and online fashion that would ensure and enhance the quality education for all, thus showing the pathway to ubiquitous learning in India.[19] Under these circumstances, the question is to ascertain the digital competence of the rural students to access these digital technologies. The objectives of this study were to examine (i) whether the rural students were ready to embrace technology in HEIs? (2) How did they perceive their readiness to receive ICT-based instruction? (3) What are their observed technological practices in enhancing themselves as being ICT-based students?

The present study is an attempt to assess the digital competence of the rural students enrolled in higher education on their readiness towards accepting digital technology i.e. the ability to understand and appreciate digital technology in education. The assessment is done using the conceptual framework as described by the European Commission in the form of the Digcomp Framework described here in the following section.

3.1. DIGCOMP: The conceptual reference model framework

The DIGCOMP framework developed by European Commission is chosen to assess the digital competence of rural students. The framework has been based on extensive study of different frameworks globally. According to its guidelines, DigComp originated from the study of many ongoing initiatives for the development and assessment of ICT skills in Europe, and to encourage their evolution. The framework serves as a

[19] Sampath (n 4).

comprehensive literature on assessment of citizens' digital competence. At the same time, DigComp aims to help citizens understand what digital competence can mean for them today, by providing an articulate and well-structured framework that describes this domain. The framework has divided the competence into five broad areas – Information; Communication; Content-creation; Safety and Problem-solving, which are further expanded to 21 competences. Each of the 21 competences is provided with eight levels of proficiency under foundation, intermediate and advanced level. The competences are also supported with examples of the related knowledge, skills and attitudinal changes and accomplishments that are desirable. It defines digital competence as a necessary element of life skills that are required for lifelong learning.[20] In comparison to this framework, the 'Digital India' program lacks a sufficient framework for judging the digital capabilities of its citizens. The DIGCOMP framework competence areas and competences can be used as a guide to characterise the digital competence profiles of groups and individuals.[21] The distinguishing feature of this framework is that it focuses more on the critical aspect of retrieving information and also on the risks of internet. Academic Literature points to the relevance of these parameters in the Indian context. For instance, a study on e-governance initiatives in the Indian state of Maharashtra points to a huge lack of people with relevant qualifications and experience to implement and man e-governance projects in the state.[22]

A short description of these competence areas and their descriptors under each area is enumerated below:

i. Information and data Literacy**:** Identify, locate, retrieve, store, organize and analyse digital information, judging its relevance and purpose

i a. Browsing, searching and filtering information

i b. Evaluating information and data

i c. Storing and retrieving information and data

[20] Khokhar (n 3).

[21] G. Evangelinos and D. Holley, 'A Qualitative Exploration of the EU Digital Competence (DIGCOMP) Framework: A Case Study Within Healthcare Education' in G. Vincenti, A. Bucciero and C. Vaz de Carvalho (eds), *E-Learning, E-Education, and Online Training* (Springer 2014) (doi:10.1007/978-3-319-13293-8_11) 85-92.

[22] Laxman L. Kumarwad and Rajendra D. Kumbhar, 'E-Governance Initiatives in Maharashtra (India): Problems and Challenges' 2016 8 (5) International Journal of Information Engineering and Electronic Business (DOI: 10.5815/ijieeb.2016.05) 18-25.

ii. Communication:- Communicate in digital environments, share resources through online tools, link with other and collaborate through digital tools, interact with and participate in communities and networks, cross-cultural awareness:

ii a. Interacting through digital technologies
ii b. Sharing information and content through digital technologies
ii c. Engaging in citizenship through digital technologies
ii d. Collaborating through digital technologies
ii e. Netiquette
ii f. Managing digital identity

iii. Content creation:- Create and edit new content (from word processing to images and video); integrate and re-elaborate previous knowledge and content; produce creative expressions, media outputs and programming; deal with and apply intellectual property rights and licences:

iii a. Developing content
iii b. Integrating and re-elaborating
iii c. Copyright and licences
iii d. Programming

iv. Safety:- Personal protection, data protection, digital identify protection, security measures, safe and sustainable use:

iv a. Protecting devices
iv b. Protecting personal data and privacy
iv c. Protecting health and well-being
iv d. Protecting the environment

v. Problem solving:-To understand where one's own digital competence needs to be improved or updated. To be able to support others with their digital competence development. To seek opportunities for self-development and to keep up-to-date with the digital evolution:

v a. Solving technical problems
v b. Identifying needs and technological responses
v c. Creatively using digital technologies
v d. Identifying digital competence gaps

4. Methodology

This paper documents a quantitative exploratory study of the readiness of rural students enrolled in Higher Education based on the questionnaire developed on the competence areas of DIGCOMP framework. The questionnaire is the main instrument of the study. Questionnaire is designed on the 21 themes of competence areas of the DIGICOMP framework. The questionnaire acts as a self-assessment tool to develop an understanding of digital competence, and its components (knowledge, skills and attitudes).

The questionnaire has been administered to the students of rural universities/colleges set up in rural India and this constituted the participant group. Survey method has been used to conduct the study.

4.1. Demographic information of respondents

A structured questionnaire on the DIGCOMP themes was sent to the participants who were from the rural campuses of Maulana Azad National Urdu University, University of Burdwan, Visva Bharati and Rayalseema University.

The number of graduate student responses was taken as 266. Out of these 266 students who responded to the questionnaire on digital competence, 62% were females and 38% were males. The girls were mostly pursuing B.Ed. Course and most of the students were from the undergraduate courses.

4.2. Use of digital devices

The survey reflects that the rural students have access to smart phones and that the digital divide has narrowed relating to access. This development is an eye opener in the sense that the access to digital technologies in rural areas has been achieved wholly contrary to rhetoric of digital divide. Figure 2 depicts their proficiency level; students knew the basics (terminology, navigation, functionality) of digital devices and used it for elementary purposes. However, they use it in everyday life and use simple content. Most of the rural students were, however, not aware of the Massive Online Open Courses or Open Education Resources. Figure 2 also suggests there is a minority population of respondents who do not own a digital device; some students are completely disengaged from technologies and involving them in the use of technology might prove really difficult.

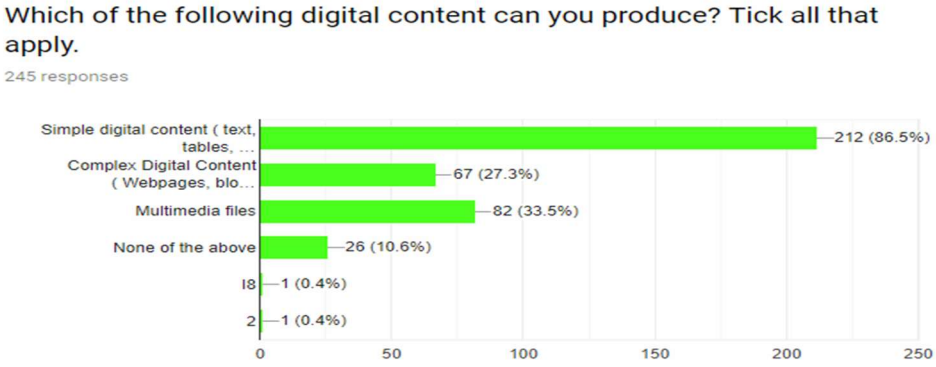


Figure 2: Extract of questionnaire

5. Data Analysis

5.1. Information and data literacy

Participants report knowledge of digital skills to retrieve information from various digital sources. Most of the rural students are comfortable using the mobile phones and use this as a medium; rather than laptops or computer. However, as per the data shown below, most of them are novice in retrieving information and majority lack skills to filter information according to their need. Many however, do not possess the skills to carry out information searches successfully and they seek the support of Library personnel for the required information. A few of the students have the ability to recognise the need for information and have the ability to locate the needed information but are beginners and do not quite know how to evaluate, only 10% have the skills to interpret the gathered information with respect to its authority, usefulness and authenticity. Significant few participants are competent in developing search strategies and are able to classify and store the gathered information for future use.

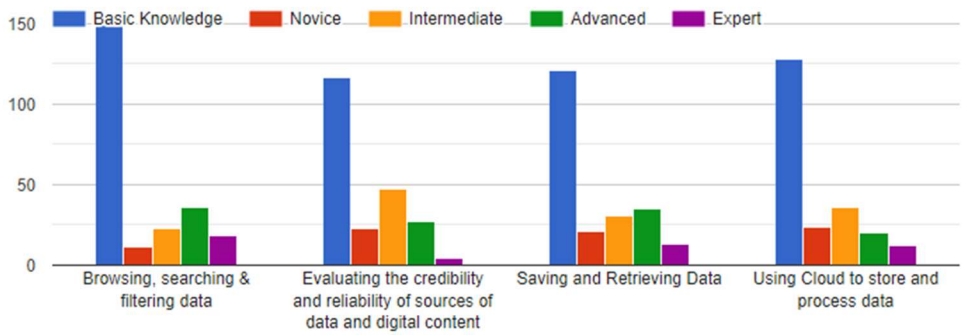


Figure 3: Levels of Proficiency

5.2. Communication and Collaboration

Communication is defined as communicating, sharing resources, linking and collaborating, interacting, facilitating cross-cultural awareness and participating in communities and networks by the utilisation of digital technologies. Participants in this competent area are questioned on these themes. The rural students use technologies that include voice calls, mobile texting, and instant messaging. The prevailing reasons are practicality, ease-of-use and cost. Only a few use skype or audio-video conferencing. The results reflected that the students are more comfortable on social networking sites. Of the total students 85% were active on social networking confirming the fact that the students used digital technologies for social purposes than academic purposes (Fig 4). Rural students are also not comfortable with mobile apps which provided services and thus do not engage in citizenship (Fig 5). They are sceptical to use the money transfer apps and preferred depositing fees in person. Majority of the respondents are not aware of the web portals and institutional repositories. It is thus concluded that the rural students use the mobile to connect with friends and for entertainment in their day to day life.

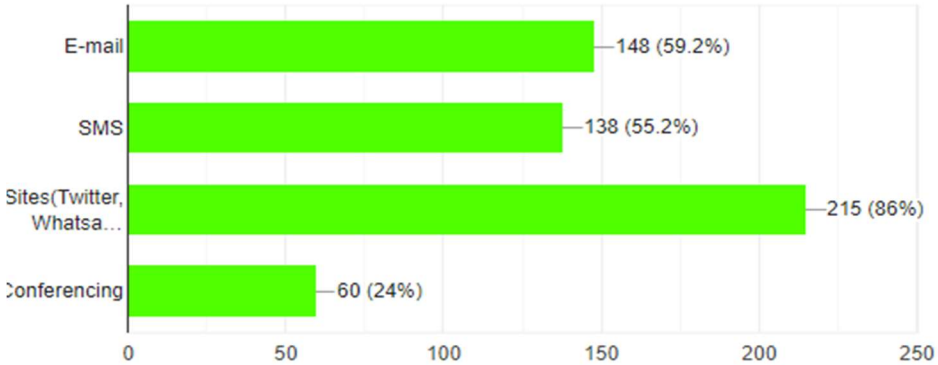


Figure 4: Medium of digital communication used by rural students

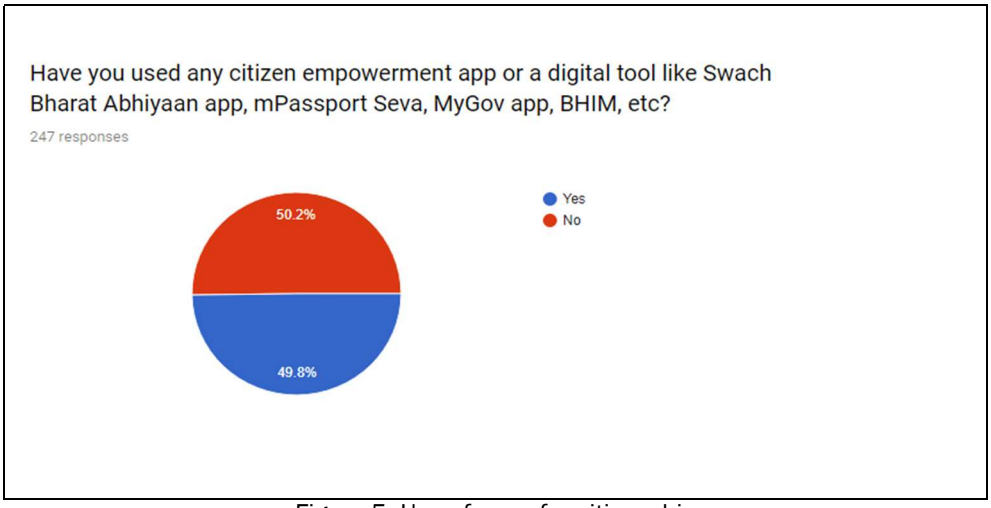


Figure 5: Use of apps for citizenship

5.3. Digital Content Creation

The 'Content Creation' definition includes the creating and editing of multimedia content, appropriating and remixing of existing content, producing creative expressions such as media artefacts and programming, dealing with and applying intellectual property rights and licencing.

Digital Literacy has bought on a new type of reading. For example, Blogs, Wikipedia entries allow and encourage the reader to become an author.

According to Rainie many students become writers when they respond on e-mails, send SMS and participate in social networks.[23]

In this study, the results of the survey show that although majority of the respondents could produce simple digital content, 27% of the respondents are familiar with wikis and blogs and can produce content on this platform. This result showed that learning to use technology has eased and rural students are adequately competent to grasp technology as depicted in figure 6.

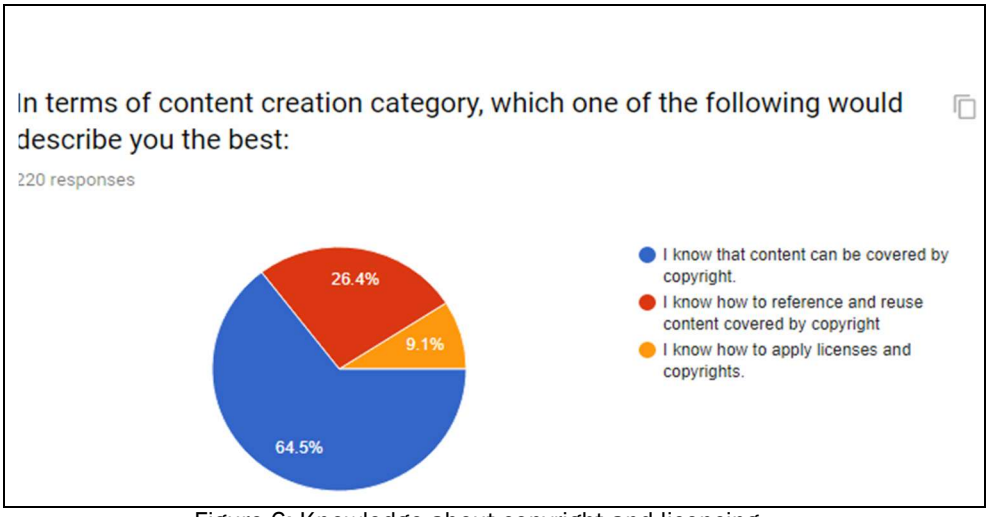


Figure 6: Knowledge about copyright and licencing

5.4. Safety

Safety has been defined as protecting personal information including digital identity and data, taking security measures in the digital environment and safety, and sustainability when using digital technologies (DIGCOMP). The questionnaire includes questions on the above themes of the safety competence. The respondents were generally aware of protecting their device and knew the use of passwords. The health aspects of using digital technology safely includes right posture, positioning, size of screen, keyboard layout, foot rest, use of light, document holder and hearing protection, just to name a few. Figure 7

[23] Quoted by Ferrari, 2011

depicts that 40% of the students were aware of the health risks associated with the use of digital technology (e.g. risk of addiction).

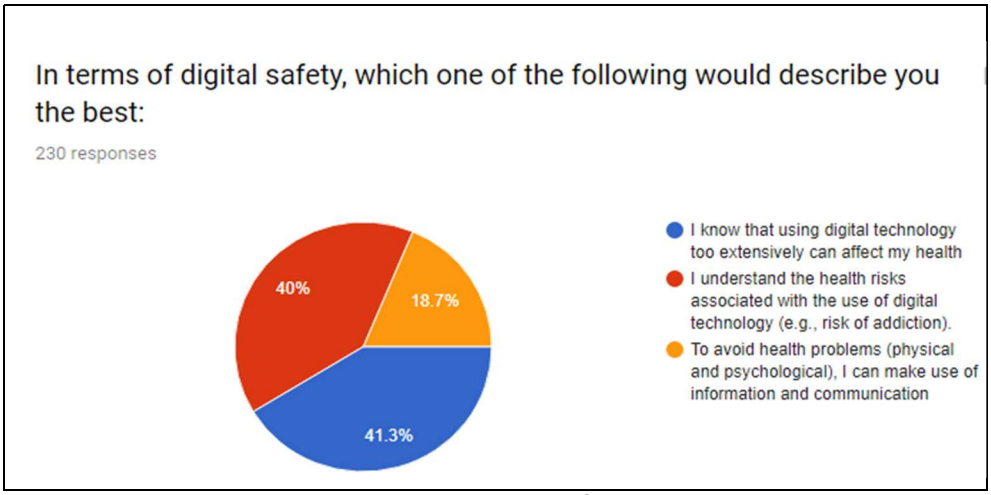


Figure 7: Digital safety

5.5. Problem –Solving

The 'Problem Solving' competence area has been defined as the identification of digital needs and resources, making informed decisions on digital tools, solving problems by utilising digital technologies, creatively using technologies, solving technical problems and updating one's own and other's digital competences. The survey on this competence depicted a median range of proficiency among students. However, one has to keep in consideration the fact that this questionnaire is a self-assessment tool, and students could have misjudged their ability to use ICT and have over-estimated their true proficiency level. Evidence from other studies shows that student's use of ICT is more a result of digital access than digital competence. Participants have also reported that they get to know about new technologies mainly from friends and family or word of mouth. Likewise when they are stuck in problem related to technology they take help from friends and overcome the challenges of technology. It was also learnt through the student's responses that they have knowledge about hardware and software in technology but admitted that they could not describe the differences in functionality, troubleshoot or differentiate potential faults.

6. Findings

- It has been learnt that the ICT tools that is best suited for rural India is the mobile. Mobiles are cheaper than PC, more portable with extended battery life suited to regions even where electricity supply is erratic. The infrastructure needed to connect wireless devices to the Internet is easier and less expensive to build. There are no costly and burdensome applications to load, maintain and update. Thus, mobile is best suited for rural India to inculcate ICT in education.
- As regarding their digital competence level, reliance on mobile technology and its applications like e-mail, and social networking apps have made the students e-ready for technology in education. Internet access and their day to day engagement with mobile based apps can be harnessed for enhanced performance in academics too.
- One of the important findings is that the digital divide between urban and rural students has narrowed. Digital devices are becoming embedded in lives of rural students as much as urban students.
- The survey on digital competence of rural students has given an opportunity for HEIs to build upon the student's social media experience. The usage of digital device for learning is minimal as depicted by the survey. Students could be encouraged to access OER and e-learning platforms to enhance their educational knowledge.
- The results of the study also shows that the students' perception of the level of their digital competence is higher than actual. Students are confusing their digital media skills with the skills required for accessing relevant information for education on all five competence areas of DIGCOMP.
- To conclude, the overall general competency levels of rural students in the selected HEIs are somewhat low for successful adoption of ICT for teaching and learning. However, it is recommended that digital competency development of rural students become an educational priority before launching ICT schemes like SWAYAM for education sector since it has a great potential even in rural areas. It would further assure inclusiveness

in terms of access and achievement of quality higher education irrespective of the locational disparity.

7. Conclusion

It is predicted that 26 billion devices will be connected to internet by 2020 confirming the wide-spread diffusion of ICT. ICT has also revolutionized the delivery of education, allowing access to higher education for greater numbers of students at lower cost and with more flexibility. In this landscape there is a need for students (future citizens) to acquire digital competence for personal development, active citizenship, social inclusion and employment. It was presumed before the study that there was a restrained access to digital devices in the rural sector. However it was interesting to note that almost all rural students were using smart phones and had experimented it for social entertainment and connecting with friends. We can therefore conclude from the study that the digital divide on access has narrowed between urban and rural students. However, due to the lack of awareness, the right skills and attitudes have not been developed in rural students to garner benefits of technology in education. It is therefore recommended that digital competency be developed and assessed on all competence areas for optimal utilization of opportunities arising due to diffusion of ICTs in higher education. This will not only help in coping with advancement of technology but also help in ending the urban rural digital divide.

References

- Ala-Mutka, K., 'Mapping Digital Competence: Towards a Conceptual Understanding' (2011) European Commission JRC 67075
- Alkali, Y. E. and Amichai-Hamburger, Y., 'Experiments in digital literacy' 2004 7 (4) Cy-berPsychology & Behavior (doi:10.1089/cpb.2004.7.421 PMID:15331029) 421–429
- Barret, A. M., 'The Education Millennium Development Goals Beyond 2015: Prospects for Quality and Learners, EdQual Working Paper No. 13, 2009.
- 'Council Recommendation of 19 December 2016 on Upskilling Pathways: New Opportunities for Adults' [2016] OJ C484/1

- Eshet, Y., ‘Digital literacy: A new terminology framework and its application to the design of meaningful technology-based learning environments’ (2002) ERIC Paper 143
- Belshaw, D. A. J., ‘What is 'digital literacy'? A pragmatic investigation’ (Durham University 2011)
- European Commission, ‘Europe 2020. A strategy for smart, sustainable and inclusive growth’ COM(2010) 2020 final
- Evangelinos, G. and Holley, D., ’A Qualitative Exploration of the EU Digital Competence (DIGCOMP) Framework: A Case Study Within Healthcare Education’ in Vincenti, G., Bucciero, A. and Vaz de Carvalho, C. (eds), *E-Learning, E-Education, and Online Training* (Springer 2014) (doi:10.1007/978-3-319-13293-8_11) 85-92.
- Evangelinos, G. and Holley, D., ‘A Qualitative Exploration of the DIGCOMP Digital Competence Framework: Attitudes of students, academics and administrative staff in the health faculty of a UK HEI’ (July, 2015) EAI Endorsed Transactions on e-Learning, (DOI=10.4108/el.2.6.e1) 2, 6
- Ferrari, A., ‘Digital Competence in Practice: An Analysis of Frameworks’ (2012) European Commission JRC 68116
- Gallardo-Echenique, Eliana; Minelli de Oliveira, Janaina; Marqués-Molias, Luis and Esteve-Mon, Francesc, ‘Digital Competence in the Knowledge Society’ (2015) 11 MERLOT Journal of Online Learning and Teaching 1-16
- Hatlevik, O. E.; Guðmund G. B. and Loi, M., ‘Examining factors predicting students’ digital competence’ (2015) 14 Journal of Information Technology Education: Research 123-137
- Khokhar, Amit Singh, ’Digital Literacy: How Prepared Is India to Embrace It?’ 2016 7 (3) International Journal of Digital Literacy and Digital Competence 1-12
- Kumarwad, Laxman L. and Kumbhar, Rajendra D., ‘E-Governance Initiatives in Maharash-tra (India): Problems and Challenges’ 2016 8 (5) International Journal of Information En-gineering and Electronic Business (DOI: 10.5815/ijieeb.2016.05) 18-25.
- Lankshear, C. and Knobel, M., *Digital Literacies – Concepts, Policies and Practices* (Peter Lang 2008)
- Ministry of Communications and Information ‘Preparing our people for digital future’ <https://www.mci.gov.sg/wps2017>

- OECD, *PISA 2009 Results: What Students Know and Can Do. Students performance in reading, mathematics and science* (vol. 1, OECD 2010)
- Pegu, U. K., 'Information and Communication Technology in Higher Education in India: Challenges and Opportunities' (2014) 4 International Journal of Information and Computation Technology 513-518
- Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning. OJ L 394, 30.12.2006, 10–18
- Sampath Kumar, B. T.; Basavaraja, M. T. and Gagendra, R., 'Computer literacy competencies among Indian students: the digital divide' (2014) 3 Asian Education and Development Studies <http://dx.doi.org/10.1108/AEDS-03-2014-0007> 267-281
- Sampath Kumar, B.T. and Shiva Kumara S.U., ' The digital divide in India: use and non-use of ICT by rural and urban students' 2018 World Journal of Science, Technology and Sustainable Development <https://www.emerald.com/insight/content/doi/10.1108/WJSTSD-07-2017-0021/full/html?fullSc=1&mbSc=1>
- Selwyn, N. 'The use of computer technology in university teaching and learning: a critical perspective' 2007 23 (2) Journal of Computer Assisted Learning (doi:10.1111/j.1365-2729.2006.002)
- Vuorikari, R.; Punie, Y.; Carretero Gomez, S. and Van den Brande, L., 'DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: The Conceptual Reference Model' (2016) European Commission JRC 27948

Short biography of the author

Neera Chopra is a PhD candidate in the Faculty of Science of Public Governance and Administration, National University of Public Service,

Budapest. She is employed in UGC, a regulating body on Higher Education in India. Her research focus is on Higher Education in India.

Electronic Commerce in Gaming Industry. European Perspective on the Legal Regulations of in-game Virtual Transactions

Olena Demchenko*

Abstract: Present paper explains the need and possible legal approach to the End User License Agreements regulating the transactions inside video games, particularly, focusing on the purchase of intangible items online for the "real life" money. This article answers two main question: why e-commerce rules should be applied to the in-game transactions and why intellectual property law rules are not enough to protect interest of both developers and users. The research focuses on gaps in existing legal procedures regulating (or not regulating) virtual transactions, stresses on the necessity of new legal models' application in gaming industry and underlines the importance of amendments to current European legislation with the focus on video games commoditization in order to protect consumer rights, free movement of digital goods and to secure Digital Single Market Strategy of the European Union.

Keywords: video games, electronic commerce, consumer protection, EULA.

1. Introduction

Since 1961, when MIT student Steven Russel created the first-ever video game "Spacewar", which inspired the further appearance of such popular video games as "Asteroids" and "Pong",[1] gaming industry went much further. Nowadays almost every electronic device has access to the Internet and both online and offline video games.

Together with the technological development and the new ways of concluding the contract being available, electronic commerce (e-commerce) in gaming industry became more sophisticated involving

* PhD student, University of Pécs, Faculty of Law, olenademchenkomail@gmail.com.

[1] A. Ramos, L. López et al., 'The Legal Status of Video Games: Comparative Analysis in National Approaches' (World Intellectual Property Organization, 2013) <http://www.wipo.int/export/sites/www/copyright/en/activities/pdf/comparative_analysis_on_video_games.pdf> accessed 24 October 2018, 7.

digital assets and a purchase of intangible virtual items. At the same time, most of the European e-commerce regulations are focused only on traditional online shopping. It seems that European regulations in gaming industry stop being valid after the purchase of a gaming software, however, considering current situation on the market such limited approach is against the real need and leaves millions of consumers (only in 2016 in Europe were counted 338 millions of players[2]) unprotected. Therefore, the present paper will focus on legal challenges arising with the application of existing e-commerce legal frames to the gaming industry.

Transactions in gaming industry can involve significant amounts of money, which does not end with the purchase of gaming software. Different types of video games are available on the market, including free-to-play (software is free, but the company gets revenue from in-game micro-transactions[3]) and pay-to-play (where player pays for software in order to access the game[4]) video games. According to the statistics, only in 2016 the total revenue in Europe from free-to-play video games reached 2 900 millions of U.S. dollars and 642 millions of U.S. dollars from pay-to-play video games[5].

Free-to-play video games bring the majority of the annual revenue to the video game companies, as players are attracted with possibility of playing without paying for the software, but during the game players are seduced with purchases of virtual items with functional (for example, virtual weapon) and without functional assistance (for example, so-called "skin") to the game. Usually such transactions require insignificant amount of money (micro-transactions)[6] and, therefore, the player does not see or cannot estimate the total cost of a video game, which can raise a question from consumer protection perspective.

[2] '2019 Video Game Industry Statistics, Trends & Data' (WePC, June 2019) <https://www.wepc.com/news/video-game-statistics/#video-gaming-industry-overview> accessed 20 June 2019.

[3] Myriam Davidovichi-Nora, 'Paid and Free Digital Business Models. Innovations in the Video Game Industry' (2014) Digiworld Economic Journal, no. 94 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2534022> accessed 20 June 2019, 87.

[4] ibid 85.

[5] '2019 Video Game Industry Statistics' (n 2).

[6] Davidovichi-Nora (n 3) 88, 94.

Notwithstanding mentioned above, not all transactions inside free-to-play video games bear insignificant character. In the Entropia Universe video game, an item, "Club Neverdie", was sold for 635,000 U.S. dollars, in "Second life" game, a virtual city of Amsterdam was sold for 50,000 U.S. dollars to the consumers[7]; in the Dota 2 video game, a player spent 38,000 U.S. dollars for "Ethereal Flames Pink War Dog" item[8]. In 2010 the most expensive video game item ever – virtual planet Calypso – was sold for 6 million U.S. dollars in Entropia Universe video game, which for now stipulates Guiness World Record[9].

Considering mentioned above, e-commerce in gaming industry shows significant turnover, however, there are no specific e-commerce rules, which can be adopted to the virtual items purchase in video games, as still nowadays all legal regulation considering video games end up on intellectual property law approach. At the same time, most of existing e-commerce regulations cannot be applied due to the specific features of certain games.

Considering significance of transactions in video game industry on the intangible items purchase, there is an urgent need to adopt existing rules in order to protect consumer rights in gaming industry and to secure Digital Single Market policy of the EU. Present paper will analyze legal challenges arising in the connection with the application of intellectual property rules, contract or property law to in-game transactions and will show possible ways to amend the rules regulating e-commerce in connection to commoditized free-to-play video games.

[7] News Report, 'Top 10 Most Expensive Virtual Items In Game Ever Sold' (GadgetRoyal, 2018) <https://www.gadgetroyal.com/top-10-most-expensive-virtual-items-in-game-ever-sold/> accessed 24 October 2018.

[8] ibid.

[9] ibid; Guiness World Record <https://www.guinnessworldrecords.com/world-records/92207-most-valuable-virtual-object> accessed 24 October 2018.

2. Legal Approach to the Developer vs User Relationships

2.1. Current Regulation on in-game Transactions

Nowadays virtual property rights are managed within the framework of the intellectual property rights protection[10]. Video game providers bind their users with so-called "Terms of Service" or "End User License Agreement" (EULA), which regulates not only behavior of the user in the game, but in many cases as well grants transfer of intellectual property rights for items created by the user in the virtual environment and all property rights outside of the game for virtual objects purchased in the game by the user[11].

Therefore, virtual items, including virtual in-game currency, which were created by the video game company (the developer) are usually considered as intellectual property of this company. For example, according to EULA of the Rocket League video game company, the trader:

> "...hereby grants you the nonexclusive, non-transferable, non-sublicensable, limited and revocable right and license to use Virtual Currency and Virtual Goods obtained by you for your personal non-commercial gameplay exclusively within the Software. Except as otherwise prohibited by applicable law, Virtual Currency and Virtual Goods obtained by you are licensed to you, and you hereby acknowledge that no title or ownership in or to Virtual Currency and Virtual Goods is being transferred or assigned hereunder. This

[10] J. Fairfield, 'Virtual Property' (2005) 85 Boston University Law Review (Indiana Legal Studies Research Paper, No. 35) <https://ssrn.com/abstract=807966> accessed 2 November 2018, 1050; J. Z. Gong, 'Defining and Addressing Virtual Property in International Treaties' (2015) 17 Boston University J. SCI. & TECH. L. <https://www.bu.edu/jostl/files/2015/02/Gong_Web_171.pdf> accessed 02 November 2018, 20; J. Stein, 'The Legal Nature of Video Games – Adapting Copyright Law to Multimedia' (2015) 2 (1) Press Start <https://press-start.gla.ac.uk/index.php/press-start/article/view/25/11> accessed 3 November 2018, 44.

[11] N. Volanis, 'Legal and policy issues of virtual property' (2007) 3 (2) Katholieke Universiteit Leuven, Int. J. Web Based Communities<https://www.law.kuleuven.be/citip/en/archive/copy_of_publications/91206-volanis2f90.pdf> accessed 28 October 2018, 334.

Agreement should not be construed as a sale of any rights in Virtual Currency and Virtual Goods."[12]

The gaming company provides no property rights to virtual goods created, purchased or obtained on the video game platform by user. Moreover, on conditions usually prescribed in the EULA, the developers can on their own consideration delete purchased property or exclude player from the game[13]. When the player spends 6 million U.S. dollars for a virtual item (example discussed above), and such player is facing the risk of being deleted from the game, the risk of non-delivery of item and the risk of the destruction of such item due to event in the game or sole decision of the developer. Such situation can be considered as a violation of consumer rights and e-commerce regulations.

In Eve Online video game, one virtual space battle, caused by the delay of the payment in "real life" money by one player needed to protect his spaceship, resulted an estimate loss of 300,000 U.S. dollars for different consumers[14]. As it can be seen, in free-to-play video games it can be not only possible to spend money, but also required to buy virtual items in order not to suffer loses in the game.

Nowadays in-game virtual property relationships are limited not only to the developer vs player relationships. There are many new businesses operating on the gaming market – third parties, which are selling items on intermediary platforms for particular video games; or third parties, which connected by agreement with a gaming company in order to provide online platform for users to play particular game. In this cases player is limited by several EULAs from different trader, which can conflict one with another.

Besides virtual items transactions leaded by video game companies, companies trading virtual assets were created following the demand. On

[12] EULA of the RocketLeague <https://www.rocketleague.com/eula/> accessed 21 April 2019.

[13] News Report, 'China's first 'virtual property' insurance launched' (China Daily, 2011) <https://kotaku.com/5818906/china-launches-virtual-property-insurance> accessed 2 November 2018.

[14] News Report 'Eve Online virtual war 'costs $300,000' in damage' (BBC News, 2014) <https://www.bbc.com/news/technology-25944837> accessed 28 October 2018.

Markee Dragon or G2G web-site it is possible to purchase so-called game-codes, which are virtual items (both functional and not) used in variety of different video games, including in-game tokens[15], for example, on mentioned platforms it is possible to purchase:

a) 750 gold crowns of the obsidians[16] (in-game money from the Shroud of the Avatar video game) for 10 US dollars or 500 PLEX (in-game money from the EVE Online video game) for 19.99 US dollars[17],
b) A virtual horse from Crowfall video game for 30 US dollars[18],
c) A noble founder's pack (skin for Legends of Aria video game) for 39.99 US dollars [19],
d) Defiant Vented Lightsaber (weapon for Star Wars: TOR video game) for 8.21 US dollars[20].

Most of the virtual items are created on virtual platforms by the developer and exist only on this virtual platforms, however, in some video games virtual items can be created by users (for example, skins) or third parties (market places for virtual items). When user spends significant amount of money for the licensing payment for the virtual item (intellectual property) and its functions or appearance is not as expected, or due to the error in the code or actions of the developer (planned event in the video game scenario) such property was destroyed, in this case regulating virtual property issues only by intellectual property law and EULA cannot be considered as a fair treatment. Therefore, different approach towards virtual property in gaming industry should be accepted by the European legislator in order to protect the rights of consumers.

[15] Information on MarkeeDragon items for purchase <https://store.markeedragon.com> accessed 21 June 2019, information on G2G items for purchase <https://www.g2g.com> accessed 21 June 2019.

[16] MarkeeDragon (n 15).

[17] ibid.

[18] ibid.

[19] ibid.

[20] G2G (n 15).

2.2. Doctrine View on in-game Transactions

Standard EULA has mixed nature involving characteristics of different types of contracts. EULA can include instruments transferring property, license on intellectual property rights and characteristics of a purchase or service provision agreements, therefore, during the practical legal application different views on the governing law are possible[21]. Present chapter will provide an overview on possible approaches to EULAs of gaming industry.

2.2.1. "No Legal Intervention" Approach

Nowadays all in-game transactions are left out of the scope of the legal regulation. Such transactions are regulated by the terms of standard EULAs, which, basically, protect only interests of the developers and leave interests of players without proper attention.

Notwithstanding, some authors argue, that the virtual reality issues should not be governed by the law at all, as players use video games in order to escape from reality[22] and many actions, which are allowed in a video game, are forbidden by the law in the "real life" world, for example, robbery or destruction of virtual property[23].

However, such approach cannot be considered as sufficient one, as virtual property bears intangible character and cannot have the same treatment as tangible items. Obviously, for in-game actions, which are prescribed by the game properties or the scenario, no one can be punished by the law (players), however, the gaming company (the developer) should be liable for non-conformity of digital goods (specific code, which is a virtual item purchased by the player), non-delivery of such

[21] Ch. Mulligan, 'Licenses and the Property/Contract Interface' (2017) Brooklyn Law School, Legal Studies Paper, No. 544 <https://ssrn.com/abstract=2987325> accessed 29 June 2019, 3.

[22] J.W. Nelson, 'The Virtual Property Problem: What Property Rights in Virtual Resources Might Look Like, How They Might Work, and Why They Are a Bad Idea' (2010) 41 McGeorge Law Review <https://www.mcgeorge.edu/documents/publications/MLR4104_Nelson_ver_09_FINAL.pdf> accessed 2 November 2018, 309.

[23] C.J. Cifrino, 'Virtual Property, Virtual Rights: Why Contract Law, Not Property Law, Must be the Governing Paradigm in the Law of Virtual Worlds' (2014) 55 (1) Boston College Law Review <https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3354&context=bclr> accessed 28 October 2018, 264.

virtual goods and for the destruction of property if it occurred due to the errors in the code.

2.2.2. Contract Law Approach

From the contract law perspective EULA is considered as mixed contract with characteristics of a license agreement and a consumer contract. EULA is a standard form contract, where the player has no power to change any of its provision and, in this case, relationships between the developer and a player bear "take it or leave it" character. When the gamer wants to play, for example, Diablo III, he has no market alternative, as every video game is a unique virtual world. The player has only one option in order to have the access to the content - to agree for standard terms EULA, which can be unfair in relation to the consumer rights for digital content. Therefore, the player has weaker position in described relationships and the player's consumer rights should be protected on the regulatory level.

Bragg vs Linden Research Inc. case, which was ruled in the U.S., can be an example of the bias character of the EULA, which includes characteristics of consumer contract and license agreement. In mentioned case the court stated that mandatory arbitration agreement, which was included in EULA, was unfair and the user in this case should be treated as a consumer[24]. In present case the court aimed to protect the rights of the consumer while signing the standard form contract (contract of adhesion according to the US law[25]) in order to play a video game.

Signing EULA in order to access free-to-play video game the player is not informed on the total price of the contract. Moreover, generally EULA neither includes provisions regarding the total price of the goods or services nor describes the manner in which the price is to be calculated, as required per Consumer Rights Directive[26].

[24] Bragg v. Linden Research Inc [2007] 487, F. Supp. 2d 593 <https://h2o.law.harvard.edu/cases/4435> accessed 29 June 2019.

[25] Cifrino (n 23) 26.

[26] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance [2011] OJ L304/64, Article 5.

Following the contract law approach, the legal regulations governing the contract law, including ones on unfair terms and consumer protection, should be applied both to the initial EULA and to agreements, where the virtual world interacts with "real life" world (virtual items purchase for "real life" money), which will be discussed in details further.

Considering mentioned above, typical EULA used by gaming companies has characteristics both of license agreement regulating copies of specific software and of consumer contract on the digital content purchase (game specific codes or so-called virtual items). Therefore, European rules regulating unfair terms, standard terms, consumer protection and conformity of digital goods should be applied to in-game transactions in the same manner as it is applied to standard consumer contracts for tangible goods (online shopping).

2.2.2. Property Law Approach

From property law perspective, video game, which allows the purchase of intangible items online for "real life" money (commoditized video game) bears the character of the contract on the transfer of property and, therefore, relevant legal provisions protecting virtual property should be applied.

Property law gives the right in rem to its holders to and such right is applicable both to tangible (for example, software on tangible media) and intangible items (for example, bank account); intellectual property law, on the other hand, gives personam rights to its holders[27].

Having a look at standard EULA, it becomes clear that the rights and obligations prescribed are neither purely in rem nor in personam[28]. Therefore, it is important to identify whether the property law elements are present in specific EULA in order to understand who has the right to protect the intangible goods in video game from third parties actions and to transfer such right. Particularly, it is important to identify so in relationships:

a) where the virtual item sold on third party platform as a "code" for a specific game,

[27] Mulligan (n 21) 4.
[28] ibid.

b) where the virtual item is sold by one user to another and it is allowed by the terms of particular EULA,
c) where the online platform for a video game is an intermediate platform between the user and a gaming company.

This mixed character of an EULA can be observed in the EULA for Second Life video game, which states, that the developer allows specific player to forbid to other players of the same video game to have access to his\her virtual real estate[29], and to trade virtual tokens (Linden dollars), which purchased in advance for "real life" money, with other users[30]. Therefore, gaming company grants intellectual property rights to unlimited amount of users and the particular user can restrict such rights to other users. From this example both in rem and personam rights can be observed. In this case, "de jure" relationships are regulated by intellectual property rights, however, "de facto" it looks like the transfer of property rights for intangible item with the right to make a decision on the property (right to sell the virtual land to another users).

Analyzing the legal doctrine on the property law it can be seen, that the property law elements are present in in-game transactions in video games.

Following Locke's view on the property rights and his labor theory, it can be concluded, that a player, who spend significant amount of time, labor, money and skills in order to achieve some fame and assets in the virtual world deserves to have the property rights for such virtual objects and avatar[31].

Following the Personhood theory, it can be observed, that in disputes over property the closest connection to the property should be prioritized[32]. Therefore, in disputes between a gaming company and a player over the avatar, the player should be favored. As example of such strong connection can be taken Jon Jacobs, known under Neverdie avatar in Entropia Universe video game. Jon "Neverdie" Jacobs opened his own

[29] EULA of the Second Life <https://www.lindenlab.com/legal/second-life-terms-and-conditions> accessed 29 June 2019, article 1.4.
[30] ibid article 3.1.
[31] Cifrino (n 23) 12.
[32] ibid 15.

company named "Neverdie"[33] selling Ethereum based Teleport tokens to be used in the virtual world[34].

Considering mentioned above, after entering the EULA in-game relationships on purchase of intangible items (game codes or so-called virtual items) between gaming company and a player bears property law character. Initial EULA grants license for intellectual property rights of some particular virtual world – right to access such virtual world and obligation not to make not licensed copies, however, in-game transaction can be considered as separate contracts on transfer of intangible goods (codes), which exist only on particular online platform, however, such codes can be traded on third party platforms or with other users.

Therefore, respective rules regulating digital content purchase and conformity of digital goods should be applied to such transactions. On the other hand, following property law view, the player should have the possibility to claim remuneration for the damages to the player's virtual property in cases, if such damages occurred not by the virtual events in the game, but by the "real life" events, for example, error in the code and breach in security of the video game. However, such legal mechanism allowing protection of virtual property is far from being available on the European market.

In some countries video game players already can protect the rights on the virtual property in the "real life" courts. In China a player whose virtual property was stolen by the hacker got remedies from the video game company in an amount equal to 1 210 U.S. dollars as a result of a court decision[35]. Moreover, a Chinese insurance company launched an insurance program in order to protect virtual property in video games[36]. In the Netherland in-game actions conducted in order to take away virtual

[33] Information on Neverdie Company <https://neverdie.com/> accessed 29 June 2019.

[34] Roger Aitken, ''President Of Virtual Reality' Behind NEVERDIE Creates Teleport Crypto Token, Raises $3.5M' (Forbes, 2017) <https://www.forbes.com/sites/rogeraitken/2017/08/02/president-of-virtual-reality-behind-neverdie-creates-teleport-crypto-token-raises-3-5m/#20a4d056273b> accessed 29 June 2019.

[35] News Report, 'Online gamer in China wins virtual theft suit' (CNN, 2003) <http://edition.cnn.com/2003/TECH/fun.games/12/19/china.gamer.reut/> accessed 2 November 2018.

[36] China Daily (n 13).

items of other players were considered as a crime (Runescape case and Habbo Hotel case)[37].

Considering mentioned above, in-game transactions on the purchase of digital content (particular code, which allows the player to obtain virtual intangible item in specific video game) should be fall under European e-commerce regulations regarding consumer protection and conformity of digital goods.

3. Conclusions

Video games, which do not allow commoditization of virtual items (pay-to-play video games) should be governed solely by the End User License Agreement, However, using the same legal approach to commoditized free-to-play video games can be considered as violation of consumer rights.

Whereas EULAs (of free-to-play video games) have mixed character of license agreements and a consumer contract, therefore, such EULAs should be tested on the subject of the unfairness of the standard form contract.

In video games, which allow the purchase of virtual intangible items (specific computer codes, which with its application to particular video game can be represented as virtual items) for the "real life" money, relevant e-commerce, consumer protection rules and rules on conformity of digital goods should be applied.

Moreover, after the specific purchase contract was concluded, such code should be protected by property law regulations in order to allow the players sell such virtual items (codes) on intermediate platform or in-game auctions and markets to another users, and to protect such virtual property from the destruction caused by "real life" events (hacking, for example).

References

– Adriaans, Tycho, 'Owning the Virtual Fruit. Protecting User Interests in Virtual Goods under Dutch Law' (Tilburg University, 2017)

[37] Tycho Adriaans, 'Owning the Virtual Fruit. Protecting User Interests in Virtual Goods under Dutch Law' (Tilburg University, 2017) <http://arno.uvt.nl/show.cgi?fid=142260> accessed 29 June 2019, 3.

<http://arno.uvt.nl/show.cgi?fid=142260> accessed 29 June 2019

- Aitken, Roger, ''President Of Virtual Reality' Behind NEVERDIE Creates Teleport Crypto Token, Raises $3.5M' (Forbes, 2017) <https://www.forbes.com/sites/rogeraitken/2017/08/02/president-of-virtual-reality-behind-neverdie-creates-teleport-crypto-token-raises-3-5m/#20a4d056273b> accessed 29 June 2019
- BBC News, 'Eve Online virtual war 'costs $300,000' in damage' (2014) <https://www.bbc.com/news/technology-25944837> accessed 28 October 2018
- Bragg v. Linden Research Inc [2007] 487, F. Supp. 2d 593 <https://h2o.law.harvard.edu/cases/4435> accessed 29 June 2019
- China Daily, 'China's first 'virtual property' insurance launched' (2011) <https://kotaku.com/5818906/china-launches-virtual-property-insurance> accessed 2 November 2018
- Cifrino, C.J., 'Virtual Property, Virtual Rights: Why Contract Law, Not Property Law, Must be the Governing Paradigm in the Law of Virtual Worlds' (2014) 55 (1) Boston College Law Review <https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3354&context=bclr> accessed 28 October 2018
- CNN, 'Online gamer in China wins virtual theft suit' (2003) <http://edition.cnn.com/2003/TECH/fun.games/12/19/china.gamer.reut/> accessed 2 November 2018
- Davidovichi-Nora, Myriam, 'Paid and Free Digital Business Models. Innovations in the Video Game Industry' (2014) Digiworld Economic Journal, no. 94 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2534022> accessed 20 June 2019
- GadgetRoyal, 'Top 10 Most Expensive Virtual Items In Game Ever Sold' (2018) <https://www.gadgetroyal.com/top-10-most-expensive-virtual-items-in-game-ever-sold/> accessed 24 October 2018
- Fairfield, J., 'Virtual Property' (2005) 85 Boston University Law Review (Indiana Legal Studies Research Paper, No. 35) <https://ssrn.com/abstract=807966> accessed 2 November 2018

- G2G, Information on G2G items for purchase <https://www.g2g.com> accessed 21 June 2019
- Gong, J. Z., 'Defining and Addressing Virtual Property in International Treaties' (2015) 17 Boston University J. SCI. & TECH. L. <https://www.bu.edu/jostl/files/2015/02/Gong_Web_171.pdf> accessed 02 November 2018
- Guiness World Record <https://www.guinnessworldrecords.com/world-records/92207-most-valuable-virtual-object> accessed 24 October 2018
- Linden Lab, EULA of the Second Life <https://www.lindenlab.com/legal/second-life-terms-and-conditions> accessed 29 June 2019
- MarkeeDragon, Information on MarkeeDragon items for purchase <https://store.markeedragon.com> accessed 21 June 2019
- Mulligan, Ch., 'Licenses and the Property/Contract Interface' (2017) Brooklyn Law School, Legal Studies Paper, No. 544 <https://ssrn.com/abstract=2987325> accessed 29 June 2019
- Nelson, J.W., 'The Virtual Property Problem: What Property Rights in Virtual Resources Might Look Like, How They Might Work, and Why They Are a Bad Idea' (2010) 41 McGeorge Law Review <https://www.mcgeorge.edu/documents/publications/MLR4104_Nelson_ver_09_FINAL.pdf> accessed 2 November 2018
- Neverdie, Information on Neverdie Company <https://neverdie.com/> accessed 29 June 2019
- Ramos, A., López, L. et al., 'The Legal Status of Video Games: Comparative Analysis in National Approaches' (World Intellectual Property Organization, 2013) <http://www.wipo.int/export/sites/www/copyright/en/activities/pdf/comparative_analysis_on_video_games.pdf> accessed 24 October 2018
- RocketLeague, EULA of the RocketLeague <https://www.rocketleague.com/eula/> accessed 21 April 2019
- Stein, J., 'The Legal Nature of Video Games – Adapting Copyright Law to Multimedia' (2015) 2 (1) Press Start <https://press-start.gla.ac.uk/index.php/press-start/article/view/25/11> accessed 3 November 2018

- Volanis, N., 'Legal and policy issues of virtual property' (2007) 3 (2) Katholieke Universiteit Leuven, Int. J. Web Based Communities<https://www.law.kuleuven.be/citip/en/archive/copy_of_publications/91206-volanis2f90.pdf> accessed 28 October 2018
- WePC, '2019 Video Game Industry Statistics, Trends & Data' (June 2019) <https://www.wepc.com/news/video-game-statistics/#video-gaming-industry-overview> accessed 20 June 2019

Short biography of the author

Olena Demchenko is a PhD student in the University of Pecs (Hungary) and a Senior Compliance Associate in Amazon Development Centre (Poland). She has international academic and work experience in Ukraine, Turkey, Hungary and Poland focusing on developments in Law and Technologies, Corporate law and Compliance.

Smart Cities, Iot and Blockchain: The Importance of Oracles

Judit Glavanits*

Abstract: The disruptive technologies like DLT (distributed ledger technology), blockchain, smart contracts and autonomous vehicles facing a common problem to solve: the collection of valid information from the "outside world". The oracles are to help in the proper functioning of these complex peer-to-peer systems, just like the in the case of autonomous vehicles. This paper examines the place of oracles (information or data providers) in the blockchain and IoV (internet of vehicles) ecosystem with a focus on responsibility of the data provided, through the glance of trust in these technologies.

Keywords: DLT, blockchain, IoT, IoV, oracles, trust

1. Introduction

Information and communication technology (ICT) is a key driver of innovation, especially in advanced economies where other sources of productivity gains has dried up or produce lower returns. As ICT helps improving access to basic services, enhancing connectivity and creating employment opportunities, ICT directly affect how people live, communicate and interact with each other.[1] For now, not only the people can communicate with each other, but also machines – even without human interaction.

The term "peer-to-peer" has come to be applied to networks that expect end users to contribute their own files, computing time, or other resources to some shared project. Even more interesting than the systems' technical underpinnings are their socially disruptive potential: in

* Associate professor, head of department, Széchenyi István University, Faculty of Law and Political Sciences, Department of International and European Law. E-mail: gjudit@sze.hu or glavanitjudit@gmail.com.

[1] World Economic Forum, *The Global Information Technology Report 2015* (2015) ICTs for Inclusive Growth.

various ways they return content, choice, and control to ordinary users.[2] It is a question however if ordinary users are capable of using this new power properly regarding to the fact that they do not necessarily understand the working method of the technology. One might say that an average user is also not in full knowledge of the technical background of the internet and still billions of us use it every day, but we should remember the first years of spreading of the net: how many failures should have happened until the regulators worldwide could create an efficient background.

The situation from the side of regulators is somehow similar today: technologies like the distributed ledger, the new currencies, possible driver-less vehicles both on the road and in the air put the decision makers into a challenging situation.

This lead us to the trust issue of the technology. Trust is not only an important basis of human interaction, but also for human-machine cooperation. The web shops and online hotel booking services are the best examples that people may rather choose a more expensive, but trusted service provider than taking the risk of trying something new. The trusted information is based on other customers' valuation, so the consumer do not need to get in touch with everybody, as many others did that before. In the IoT world however we need to build trust between devices, or at least teach (program) them how to choose to rely only on trusted sources of information.

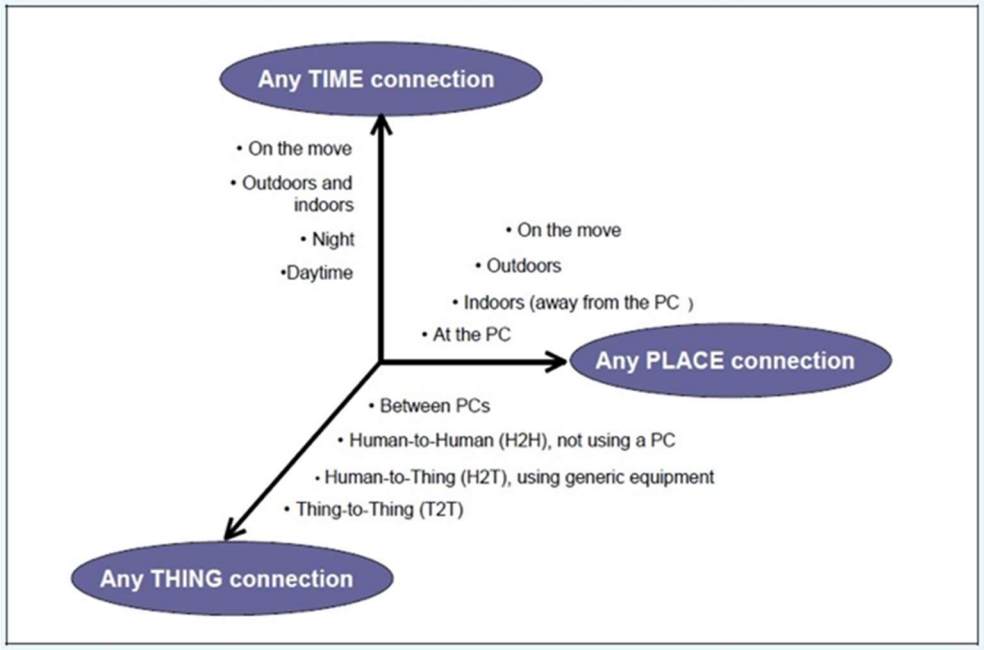
2. Basic concepts of IoT, IoV and blockchain

*Internet of Thing*s (IoT) refers to a network of items – each embedded with sensors – which are connected to the Internet.[3] In the early years of the technology the ITU (International Telecommunication Union – part of the UN) defined IoT as "*from anytime, any place connectivity for anyone, we will now have connectivity for anything*". This definition is from year 2005, still the best summary of the matrix how IoT is basically working.

Figure 1. IoT – defined by ITU in 2005 (source: ITU)

[2] Andy Oram (ed), *Peer-to-peer: Harnessing the Power of Disruptive Technologies* (1st edn, O'Reilley Media 2001) Definitions. s.p.

[3] Somayya Madakam et al., 'Internet of Things (IoT): A literature overview' (2015) 3 (5) Journal of Computer and Communications,168.



The term "Internet of Things" was introduced by Kevin Ashton in 1999 linking the new idea to RFID (radio frequency identification). As he said 10 years later: "*the problem is, people have limited time, attention and accuracy – all of which means they are not very good at capturing data about things in the real world*".[4] He suggested that if we had computers that knew everything there was to know about things – using data they gathered without any help from human beings – we could be able to track and count everything, and greatly reduce waste, loss and cost. To reach this, we need to empower computers with their own means of gathering information, so they can "see, hear and smell" the world for themselves.[5]

The network of tomorrow, built on an increasing number of sensors and thus, increasing data, will produce a hyperconnected environment or 'Internet of Things', with estimates of over 50 billion things connected by 2020.[6]

[4] Kevin Ashton, 'That 'Internet of Things' Thing' (*RFID Journal*, 22 June 2009) 1.
[5] ibid.
[6] UN-GGIM, *Future Trends in geospatial information management: the five to ten year vision* (2nd edn, August 2015).

The IoT involves a huge number of connected devices via the Internet, and creates new social, political, economic and ethical landscape. Thus, many governments accepted the fact that they have to play an active role in establishing and supporting an environment in which new technologies such as blockchain and IoT can flourish, emerge and grow.[7] In March 2015 the Alliance for Internet of Things Innovation was launched by the European Commission to support the creation of an innovative and industry driven European Internet of Things ecosystem. The European Union's IoT vision is based on three pillars: (1) a thriving IoT ecosystem, (2) a human-centered IoT approach and (3) a single market for IoT. However, the vision is easier to declare than to succeed.

According to Spyros G. Tzafestas, the IoT law and ethics framework should involve regulations for the devices connected, for the networks and for the data associated with the devices, but also should involve ethics principles rules and codes, and contractual guidelines.[8]

There are so many objects (traffic lights, cars, thermostats, refridgertors, alarm clocks, mobile phones, smart watches, surveillance cameras and so on) that the concept of IoT has moved towards "Internet of Everything". In this area, one of the most advanced business is undoubtedly the car/vehicle industry. The connecting spot leading us from IoT solutions to IoV networks is *smart city*. Smart cities add digital intelligence to existing urban systems creating a pervasive, integrated, and intelligent city environment where IoT solutions are used to seamlessly interconnect, interact, control, and provide insights about the various silos of fragmented systems within cities.[9] Currently, conventional vehicles have devices, for example, GPS, radio handset, small-scale impact radars, cameras, on-board computers and various kinds of detection devices to warn the driver of a wide range of good conditions—being of the street and mechanical breakdowns. The vehicles are more refined due to their on-board storage capacity, on-board computing capabilities, significant matching capabilities and fewer power hindrances, which are supported by sensors, actuators, radar hosts and

[7] World Bank Group, 'Internet of Things. The New Government to Business Platform' (Working Paper, 2017).

[8] Spyros G Tzafestas, 'Ethics and Law in the Internet of Things World' (2018) 1 Smart Cities, 98-120.

[9] IOT Analytics, 'Connected Streetlights 2018-2023' (Market Report, June 2018).

GPS.[10] The smart city of the future can be built on the system of IoV – discussed in the followings.

The *Internet of Vehicles* (IoV) has basically two phases of development (at least so far). As a part of IoT world, the Vehicle Ad-hoc Network (VANET) turns every participating vehicle into a wireless router or mobile node, enabling vehicles to connect to each other and in turn, create a network with a wide range. Next, as vehicles fall out of the signal range and drop out of the network, other vehicles can join in, connecting the participants to one another to create a mobile Internet. Regarding to it's limited possibilities of usage, a necessary development made it possible to turn to IoV (or what we call IoV today)[11]: an open and integrated network system with high manageability, controllability, operationalization and credibility and it is composed not only of vehicles, but of multiple users, multiple vehicles, multiple things and multiple networks.[12] There are essentially three types of vehicle connection:

(1) V2D: vehicle to device – communication between automated vehicles and different categories of devices (smart phones, watches, PC);
(2) V2I: vehicle to infrastructure – more specific type of communication between vehicles and infrastructures like traffic lights or speed cameras;
(3) V2V: vehicle to vehicle – this communication supposes fully autonomous driving or at least high level of automation.[13]

[10] Pradip Kumar Shama, Seo Yeon Moon and Jong Hyuk Park, 'BlockVN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City' (2017) 13 (1) Journal of Information Processing Systems, 184-195.

[11] For self-driving machines and their liability issues see in details: István Ambrus, Gábor Kovács and Imre Németh, 'Az önvezető járművek kapcsán felvethető általános büntetőjogi problémák' (2018) (2) JURA, 13-31 and István Ambrus, 'Az önvezető járművek várható hatása a közlekedési bűncselekményekre' (2018) (6) Ügyészek Lapja, 5-14.

[12] Fangchun Yang, Shangguang Wang, Jinglin Li and Zhinan Liu and Qibo Sun, 'An Overview of Internet of Vehicles' (2014) 11 (10) China Communications, 1-15.

[13] Maria Cristina Gaeta, 'The issue of data protection in the Internet of Things with particular regard to self driving cars' (2017) Diritto Mercato Technologia, <https://www.academia.edu/35993304/The_issue_of_data_protection_in_the_Internet_of_Things_with_particular_regard_to_self_diving_cars_2017_DIMT> accessed 09 December 2019.

In the scientific literature we can find several more types of interactions[14] and examining important connection points of IoV and blockchain technology. Some authors point out that an important social challenge for IoV technology is the appropriate rewarding of vehicle objects to serve as data mules for data collection and transportation from smart sensors.[15] A kind of extension of IoV is so-called Social Internet of Vehicles (*SIoV*), which can be described as a vehicular social network, as social interactions among cars, which communicate autonomously to look for services (automaker patches or updates) and exchange information relevant to traffic. Given that vehicles are becoming more and more autonomous, and that applications supporting social interactions among drivers and passengers are already on a higher level of development (see Waze for example), some authors strongly believe that SIoV will eventually be a network of both drivers, passengers and cars.[16]

Blockchain technology is being explored in many innovative applications, such as cryptocurrencies, smart contracts, communication systems, health care, financial systems, electronic voting, and distributed provenance - among others.[17] Using blockchain's transparent and fully distributed peer-to-peer architecture, these applications benefit from an append-only model in which transactions accepted in the blockchain cannot be modified.[18]

Blockchain technology is based on distributed ledger technology (DLT), but the two are not the same: all blockchains and DLT, but not all DLTs are blockchains. There are several types of each "product", but we can

[14] Li Ang, Kah Seng, Gerald Ijemaru and Murtala Adamu, 'Deployment of IoV for Smart Cities: Applications, Architecture and Challenges' (2018) 7 (1) IEEE Access, 6473-6492. DOI: 10.1109/ACCESS.2018.2887076.

[15] You-Chiun Wang and Guan-Wei Chen, 'Efficient Data Gathering and Estimation for Metropolitan Air Quality Monitoring by Using Vehicular Sensor Networks' (2017) 66 (8) IEEE Transactions on Vehicular Technology, 7234-7248. DOI: 10.1109/TVT.2017.2655084.

[16] Leandros A. Maglaras, Ali H. Al-Bayatti, Ying He, Isabel Wagner and Helge Janick, 'Social Internet of Vehicles for Smart Cities' (2016) 5 (1) Journal of Sensor and Actuator Networks, doi: 10.3390/jsan5010003.

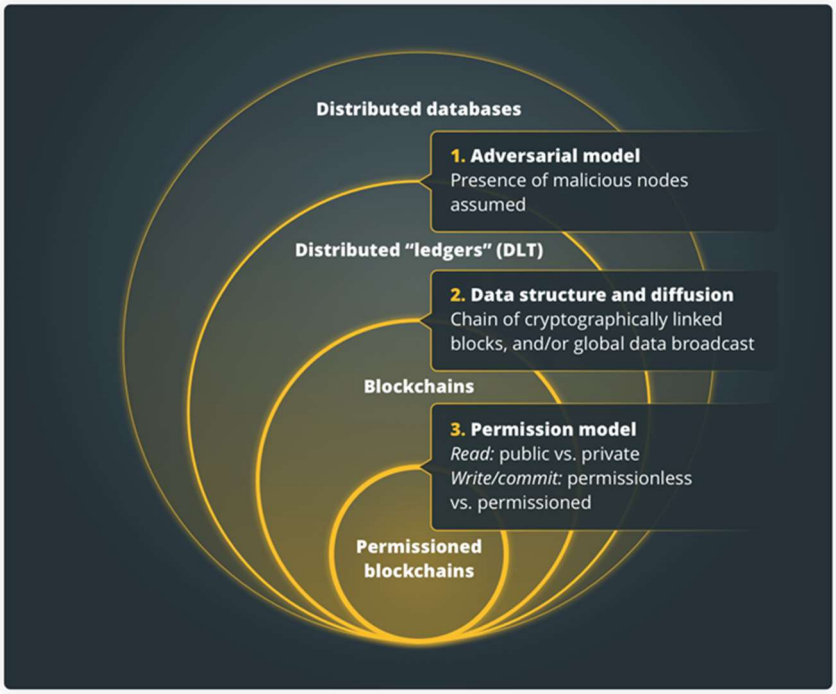
[17] See in details: Stephen P. Williams, *Blockchain: The Next Everything* (Scribner 2019).

[18] See in details e.g.: Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvardy University Press 2018) and Daniel Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Step*s (Apress 2018) and Imran Bashir, *Mastering Blockchain* (Packt 2018).

summarize some common differences that are true for most of the systems operated by blockchain or DLT technology:

(1) Blockchains are basically permission-less and open, and DLTs are basically permissioned and closed.
(2) Blockchains need miners, while there is no mining activity by DLTs.
(3) Blockchains are made of blocks, while there are no blocks on DLTs.
(4) Blockchains are fitting for cryptocurrencies, DLTs are not.
(5) Many of the blockchains enable token creation, DLTs are not capable of this.

The relationship between blockchain and DLT



cointelegraph.com source: jjablog

Common understanding of IoV and blockchain systems:

Global interest	IoT, IoV and blockchain technologies are defined only in an international manner, as the technology is only effective when there are no borders physically or financially
Autonomous	the systems basically do not require human interaction
Trust-based	The blockchain systems were created as an answer to the broken trust in the traditional banking system and IoV needs the human trust of taking the control over the driving experience.
Interconnected	Both technologies are based on the interconnected and globalized word built on the internet.
IP-sensitive	The Intellectual Property issues arouse both fields that are not necessarily solved even on national level[19], and the whole open innovation method needs more regulatory attention[20]
Lack of regulation	Unfortunatelly we can conclude that the time being both technologies need proper and future-driven regulation – hopefully – in the near future.

Let's jump into the future, and imagine a smart city, where the IoT, the IoV and the blockchain technology together enhancing the effectiveness of the everyday life:

"*Shanu gets into her car to drive to work; she is an active mother and senior director for a large corporate. The car consequently synchronizes with Shanu's smart mobile phone's SmartPay benefit, a framework that gives security and trust by "epitomizing" Shanu through smart contracts on its blockchain interface. That permits it to work as an autonomous payment device. SmartPay starts a few elements on Shanu's in-car show;*

[19] Péter Somkutas and Ákos Kőhidi, 'Az önvezető autó szoftvere magas szintű szellemi alkotás vagy kifinomult károkozó?' (2017) (2) In Medias Res, 232-269.

[20] J. L. de la Rosa, D. Gibovic, V. Torres, L. Maicher, F. Miralles, A. El-Fakdi and A. Bikfalvi, 'On intellectual property in online open innovation for SME by means of blockchain and smart contracts' (3rd Annual World Open Innovation Conference (WOIC), 2016) <https://www.researchgate.net/publication/311581389_On_Intellectual_Property_in_Online_Open_Innovation_for_SME_by_means_of_Blockchain_and_Smart_Contracts/link/584ea7b208ae4bc899395b86/download> accessed 09 December 2019.

it connections to journey planner, and Shanu goes into SmartPay travel organizer her office as her goal. SmartPay travel organizer decides, by questioning vehicle information, that the auto is low on fuel, so it consequently plots a course using an advantageous petrol station that is promoting aggressive fuel costs. In the wake of topping off with fuel consequently paid for by SmartPay's smart contact include, Shanu gets a message over the SmartPay interface that her work car stop is full and that SmartPay travel organizer has started a shrewd contract trade and paid for another car stop, a short separation from her office. While at work, Shanu gets a message that SmartShop has offered her everyday shopping rundown to neighborhood retailers, decided the one with the best costs, paid for it all, and has composed conveyance, which arrives not long after Shanu's returns home from work. Later that same night, Shanu's daughter, Zimpy, makes a request to get the car. Zimpy's smart contract with Shanu's car gives her get to. However, it does not empower the vehicle to make self-ruling installments for everything; shrewd contracts are correctly that-keen; they are adaptable for every relative. In this way, Zimpy can refuel. However, she cannot treat her companions to a drive through KFC utilizing her mom's SmartPay benefit. In addition, regardless of the possibility that Zimpy could pay for things she ought not, Shanu would rapidly discover because she would have the capacity to check the changeless exchange history on SmartPay's interface to the car's blockchain record."[21]

3. Trust – a basis for the innovative technologies

Trust plays a central role in many aspects of computing, especially those related to network use. Whether downloading and installing software, buying a product from a web site, or just surfing the Web, an individual is faced with trust issues. Trust in peer-to-peer, collaborative, or distributed systems presents its own challenges. Some systems deliberately disguise the source of data; all of the systems use computations or files provided by far-flung individuals who would be difficult to contact if something goes wrong - much less to hold responsible for any damage done.[22]

[21] Shama, Moon and Park (n 10) 190-191.
[22] Mark Waldman, Lorrie Faith Cranor and Avi Rubin, 'Trust' in Oram (n 2) 153-170.

According to McKinght[23] the overall trust concept means secure willingness to depend on a trustee because of that trustee's perceived characteristics. Three main types of applicable trust concepts are follows:

1. *Trusting beliefs* means a secure conviction that the other party has favorable attributes (such as benevolence, integrity, and competence), strong enough to create trusting intentions. Trusting beliefs-IT means a secure conviction that the technology has desirable attributes. For example, one may believe the blockchain system is recording the transaction reliable, safe, and timely in completing its task.

2. *Trusting intentions* means a secure, committed willingness to depend upon, or to become vulnerable to, the other party in specific ways, strong enough to create trusting behaviors. Trusting intention-IT means one is securely willing to depend or be vulnerable to the information technology. This is the psychological state one possesses before hitting the "Download now" button.

3. *Trusting behaviors* means assured actions that demonstrate that one does in fact depend or rely upon the other party instead of on oneself or on controls. Trusting behavior is the action manifestation of willingness to depend. Trusting behavior-IT means that one securely depends or relies on the technology instead of trying to control the technology. For example, one is using the Ethereum blockchain for smart contracting without the need to control the Ethereium network as a whole.

When the trustor has no prior interaction with a trustee, he/she cannot develop trust based on direct experience with or first-hand knowledge of the trustee. Instead, the trustor will depend on other sources, such as second-hand information, contextual factors, or personal intuition to make trust inferences. For example, before having direct interaction with an information system in a specific context, a trustor can build initial trust in this system based on their experiences with other systems, their knowledge about this system used in other contexts, and/or others' opinions about the system.[24] In case of IoT and IoV this is critical:

a. Trust in the system

[23] D. Harrison McKnight, 'Trust in Information Technology' in G. B. Davis (ed), *The Blackwell Encyclopedia of Management*. Vol. 7 *Management Information Systems* (Blackwell 2005) 329-331.

[24] Xin LI, Traci J Hess and Joseph S Valaich,'Why do we trust new tecchnology? A study of initial trust formation with the organizational information systems' (2008) 17 (1) The Journal of Strategic Information Systems, 39-71.

Trust is a basic question of IoT and blockchain systems. DLT and blockchain technology itself arouse on the grounds of distrusted banking (and financial) system and on the need to build trust between unknown business partners.

Overall, across all markets, trust in organizations' use of personal data is eroding, both in terms of security and use. An important question is whether there is a tipping point, when benefits of signing on to a service are outweighed by the risks and potential damage caused by the online presence.[25]

b. Trust in the source

Data are central to blockchain and IoT technology, but there is inconsistent understanding of data's value and management in general.[26] Data from IoT can be an economic asset for both government and businesses, and the data used by the IoT can be a question of trustworthiness for the service providers and consumers using the technology.

4. Oracles of the new technologies

The new technologies like DLT, blockchain, smart contracts and autonomous vehicles are facing a common problem to solve: the collection of valid information from the "outside world". On the field of blockchain systems the computations can only operate on data that is on the blockchain, that is, a prior computation initiated by a user on the chain wrote the relevant data into the virtual machine's memory. The network does not natively support reaching consensus on the validity of such data, only the fact that it exists on the blockchain can be agreed upon.[27] Smart contracts emerged with the rise of the blockchain technology: these agreements are encoded as a programming language code and deployed on a blockchain platform, where all participants execute them and maintain their state. To release the potential of smart contracts, it is

[25] See more on this: ITU (International Telecommunication Union), 'Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security' (2018).

[26] World Bank Group (n 7) 27.

[27] John Adler et al., 'ASTREA: A Decentralized Blockchain Oracle' (2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018) 1145-1152.

necessary to connect the contracts with the outside world, such that they can understand and use information from other infrastructures.[28]

Oracles were primarily centralized services, meaning any smart contract using such services has a single point of failure, which nullifies any benefits gained from the decentralized nature of smart contracts. However, several new developments made this possible failure less likely to happen: Chainlink for example is designed as a decentralized oracle that can provide external data to smart contracts.

Working method of Chainlink[29]

There are different types of oracles for blockchain systems, the following categorization is based on the work of Shermin Voshmgir:[30]

(1) *Software Oracles:* handle information data that originates from online sources, like temperature, prices of commodities and goods, flight or train delays, etc. The so ware oracle extracts the needed information and pushes it into the smart contract.

(2) *Hardware Oracles:* Some smart contracts need information directly from the physical world, for example, a car crossing a

[28] Juan Guarnizo and Pawel Szalachowski, 'PDFS: Practical Data Feed Service for Smart Contracts' (*ESORICS*, 2018). DOI:10.1007/978-3-030-29959-0_37.

[29] <https://docs.chain.link/docs/welcome-to-chainlink>.

[30] Shermin Voshmgir, *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy* (BlockchainHub 2019).

barrier where movement sensors must detect the vehicle and send the data to a smart contract, or RFID sensors in the supply chain industry.

(3) *Inbound and Outbound Oracles:* inbound oracles provide data from the external world, while outbound oracles provide smart contracts with the ability to send data to the outside world. An example would be a smart lock in the physical world, which receives payment on its blockchain address and needs to unlock automatically.

(4) *Consensus-based Oracles:* get their data from human consensus and prediction markets like Augur and Gnosis. Using only one source of information could be risky and unreliable. To avoid market manipulation, prediction markets implement a rating system for oracles. For further security, a combination of different oracles may be used, where, for example, three out of five oracles could determine the outcome of an event.

IoV and oracles: from weather forecast to consumer's info

As discussed earlier IoV uses (among others) V2V (vehicle-to-vehicle), V2R (vehicle-to-road), V2H (vehicle-to-human) and V2S (vehicle-to-sensor) interconnectivity, for creating a social network with intelligent objects as participants. An effective and efficient integration of existing and different network types standards are very important in the IoV ecosystem. Furthermore, the integration of cloud computing, fog computing, mobile edge computing, AI and big data analyses are all essential for an effective IoV development (Skulimowski et al. eds 2018).[31] Security in IoV becomes of paramount importance as any system failure directly affects user safety.

Data sources and security risks for IoV

			Security risk
	Cloud:	Management platform	traditional operating system

[31] Andrzej M.J. Skulimowski, Zhengguo Sheng, Sondès Khemiri-Kallel, Christophe Cérin and Ching-Hsien Hsu (eds), *Internet of Vehicles. Technologies and Services Towards Smart City: 5th International Conference, IOV 2018, Proceedings* (Springer 2018).

DATA FEED	Service Platform	Information Service Applications	risks; denial of service attacks
		Call Center Application	
		Data storage	data is falsified or tampered, individual privacy threat
	Channel: V2X Communication	V2V	wireless communication hijacking; communication protocol cracking; malicious nodes invade
		V2I	
		V2N	
		IVN (In-Vehicle Network)	
	Device: Intelligent devices Connected devices	Mobile operating system APP	APP crack: debug or decompile applications – obtain communication keys
		T-box, IVI	internal information leakage, lack of security isolations, lack of encryption and access control mechanism
		OBD Interfaces, sensors and multi-function key	Accoustic interference, radar noise attack, cameras: blinding glare

Source: based on Tian (2017)[32]

[32] Huirong Tian, 'Introduction of IOV Security' *Security Research Institute, CAICT, 2017-11-02*.

Blockchain for IoV: massage dissemination via blockchain

For a proper use of IoV and VANET systems a mass of information is required – as discussed previously. However, the traditional VANET (or IoV) faces several security issues – as shown in the previous table. Shrestha and co-authors in 2018 proposed a new type of blockchain to resolve critical message dissemination issues in VANET. They created a local blockchain for real world event messages exchanged between the vehicles, for this they created a public blockchain that stores the node trustworthiness and message trustworthiness in a distributed ledger that is appropriate for secure message dissemination.[33] This is a perfect example of how the new technologies can support the effectiveness of each other.

5. Malfunction and intentional threats, as common risks

Just as the Internet aggravated the risks of cyberwarfare, spam, identity theft, and denial-of-service attacks, connected everyday objects become targets for malicious software that causes everyday devices to fail or spy. Sensor networks become channels for unauthorized surveillance by mischief makers or criminals (National Intelligence Council 2008).[34]

Cyberattacks are increasing in terms of both scale and volume across all sectors of public and private life. A cyberattack is a malicious attempt made by an individual or organization to breach the information system of another individual or organization. Most commonly, cyberattacks target the business organization, military, government, or other financial institutions such as banking either for hacking secured information or for a ransom.[35]

[33] Rakesh Shrestha, Rojeena Bajracharya and Seung Yeob Nam, 'Blockchain-based Message Dissemination in VANET' (2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), 2018) 161-166.

[34] National Intelligence Council, 'Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests out to 2025' (SRI Consulting Business Intelligence 2008) <https://fas.org/irp/nic/disruptive.pdf> accessed 9 December 2019.

[35] A. Saravan and Sathya S. Bama, 'A Review on Cyber Security and the Fifth Generation Cyberattacks' (2019) 12 (2) Oriental Journal of Computer Science and Technology 51.

In the world of IoT, population of devices are growing, and expected to grow further rapidly, as users embrace more connected devices, more sensors are deployed, and more objects are embedded with information. Each device, depending on its type, carries with it an associated set of channels, methods, and data items, each of which is subject to potential abuse. This increased population of devices has the effect of creating an explosion in the total number of potential target resources across the Internet, as well as within any specific environment.[36]

Although blockchain technology prevents several types of malicious attacks and reduces many associated risks, it does not eliminate all attacks. Its preventative mechanisms (e.g., distributed consensus, cryptography, anonymity) may impair its resistance to other types of frauds and maliciousness- including the so called "51% attack", account takeover, digital identity theft, money laundering, and hacking.

A "51% attack" occurs when someone controls the majority of mining power on a Proof-of-Work blockchain network (like bitcoin). This means that the majority block verifier can prevent other users from mining and reverse transactions. In 2019 two major blockchains were attacked this way: (1) two miners have reportedly executed a 51% attack on the bitcoin cash (BCH) blockchain, published in May 24, however in this case happened with good intent, as the two mining pools attempted to prevent an unidentified party from taking some coins that — due to a code update — were essentially "up for grabs."[37] Earlier in January 7, the Ethereum blockchain was attacked: the incident occurred over a period of 4 hours between 0:40 and 4:20 Jan.7, 2019 UTC, during which the transactions were normally confirmed on the blockchain and then subsequently invalidated after the malign network rollback.[38] Account takeover – also known as account compromise – happens when a fraudster gets access to a genuine customer's account. Any online account could be taken over by fraudsters, including e-commerce accounts, subscriptions, banks, credit cards, emails.. etc. But the biggest problem with blockchain systems – as many of the financial supervisiory authorities believe – that

[36] See in details: Michael J. Covington and Rush Carskadden, 'Threat Implications of the Internet of Things' in Podins, Stinissen and Maybaum (eds): *5th International Conference on Cyber Conflict* (NATO CCD COE Publications 2013) 1-12.

[37] <https://cointelegraph.com/news/two-miners-purportedly-execute-51-attack-on-bitcoin-cash-blockchain> accessed 30 November 2019.

[38] <https://www.gate.io/article/16735> accessed 30 November 2019.

they can be used for money laundering as well as for legal purposes. The advent of cryptocurrency has introduced an intriguing paradox: pseudonymity allows criminals to hide in plain sight, but open data gives more power to investigators and enables the crowdsourcing of forensic analysis.[39]

6. Regulation at crossroads

The upper detailed new technologies' – especially the blockchain/ DLT technology – future depend on the national regulations. In case of IoT and IoV the responsibility issues are on the table for a couple of years now. Blockchain technology however is still in the phase of understanding: the US Congress introduced a bill to the Senate to direct the Secretary of Commerce to establish a working group to recommend to Congress a definition of blockchain technology.[40] The EU has already understood the phenomena, and on 10th of April 2018, 21 Member States and Norway agreed to sign a Declaration creating the European Blockchain Partnership (EBP) and cooperate in the establishment of a European Blockchain Services Infrastructure (EBSI) that will support the delivery of cross-border digital public services, with the highest standards of security and privacy. Since then, eight more countries have joined the Partnership, bringing the total number of signatories to 30 (status at December 2019).

Robert Ashley, Director of Defence Intelligence Agency declared in 2018, that "The most important emerging cyberthreats to our national security will come from exploitation of our weakest technology components: mobile devices and the Internet of Things (IoT)."[41]

In the USA, the country's first IoT security law is California's Senate Bill No. 327, which passed in September 2018, effective from 1st January 2020. California's law requires specific security measures that device makers have to adhere to, like getting rid of default passwords and

[39] See in details: Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl I. Weidele, Claudio Bellei, Tom Robinson and Charles E. Leiserson, 'Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics' in *Proceedings of ACM Conference* (KDD '19 Workshop on Anomaly Detection in Finance) (ACM 2019).

[40] S.553 – 116th Congress (2019-2020)

[41] <https://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/1457815/statement-for-the-record-worldwide-threat-assessment/> accessed 9 December 2019.

requiring users to generate their own passwords before allowing device access.

According to the regulation:

"*1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:*

(1) Appropriate to the nature and function of the device.

(2) Appropriate to the information it may collect, contain, or transmit.

(3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

(b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:

(1) The preprogrammed password is unique to each device manufactured.

(2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time."

Going further, the Senate is proposed a Bill on 23rd September 2019 called "Internet of Things Cybersecurity Improvement Act of 2019" or "IoT Cybersecurity Improvement Act of 2019" on the minimum security standards for IoT devices purchased by the Federal Government. Section 5 of the proposed bill contains, that the Director of the National Institute of Standards and Technology should – not later than 1 year after the passing of the Bill – propose recommended guidelines for the use of IoT devices. This guidelines should contain detailed sections on:

"*(A) receiving information about a potential security or personal information vulnerability relating to agency information systems, and when relevant, Internet of Things devices; and*

(B) disseminating information about the resolution of a security or personal information vulnerability relating to agency information systems, and when relevant, Internet of Things devices."

The European Commission stated in a working document that in case of IoT devices and systems consumers' trust and the uptake of these technologies will depend on whether they are perceived to be safe and on whether the legal framework is considered clear and effective to provide remedies to victims.[42] According to the Commission, the potential of technologies, such as blockchains or deep-learning, in the field of IoT could be further explored in the Single Market Area. "Such distributed architectures could offer alternative and more efficient ways to meet the challenges of interoperability but also of trust and data ownership/usage".[43]

Institutions like NIST in the USA, the European Telecommunications Standards Institute and the China National Institute of Standardization and also the International Standards Organization are important players in the "constitutionalization" of the Internet and the regulation of IoT. Their possible incorporation of human rights discourse in the development of national and international standards appear to establish obligations and limitations on international, national, and private actors involved in Internet platforms.[44]

References

- Adler, John et al., 'ASTREA: A Decentralized Blockchain Oracle' (2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018) 1145-1152
- Ambrus, István; Kovács, Gábor and Németh, Imre, 'Az önvezető járművek kapcsán felvethető általános büntetőjogi problémák' (2018) (2) JURA 13-31.

[42] European Commission, 'Commission Staff Working Document – Liability for emerging digital technologies' SWD(2018) 137 final.

[43] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry - Reaping the full benefits of a Digital Single Market' COM(2016) 180 final.

[44] Adam Todd, 'Using a Human Rights Framework for Regulating the Internet of Things: The Critical Role of Human Rights Advocacy' (Conference: The Social Practice of Human Rights, 2019) <https://ecommons.udayton.edu/human_rights/2019/events/61> accessed 9 December 2019, 61.

- Ambrus, István, 'Az önvezető járművek várható hatása a közlekedési bűncselekményekre' (2018) (6) Ügyészek Lapja, 5-14
- Ang, Li; Seng, Kah; Ijemaru, Gerald and Adamu, Murtala, 'Deployment of IoV for Smart Cities: Applications, Architecture and Challenges' (2018) 7 (1) IEEE Access, 6473-6492. DOI: 10.1109/ACCESS.2018.2887076.
- Ashton, Kevin, 'That 'Internet of Things' Thing' (*RFID Journal*, 22 June 2009)
- Bashir, Imran, *Mastering Blockchain* (Packt 2018)
- Covington, Michael J. and Carskadden, Rush, 'Threat Implications of the Internet of Things' in Podins, Stinissen and Maybaum (eds): *5th International Conference on Cyber Conflict* (NATO CCD COE Publications 2013)
- De Filippi, Primavera and Wright, Aaron, *Blockchain and the Law: The Rule of Code* (Harvardy University Press 2018)
- De la Rosa, J. L.; Gibovic, D. and Torres, V., Maicher L. and Miralles, F. and El-Fakdi, A. and Bikfalvi, A., 'On intellectual property in online open innovation for SME by means of blockchain and smart contracts' (3rd Annual World Open Innovation Conference (WOIC), 2016)
- Drescher, Daniel, *Blockchain Basics: A Non-Technical Introduction in 25 Step*s (Apress 2018)
- European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry - Reaping the full benefits of a Digital Single Market' COM(2016) 180 final
- European Commission, 'Commission Staff Working Document – Liability for emerging digital technologies' SWD(2018) 137 final
- Gaeta, Maria Cristina, 'The issue of data protection in the Internet of Things with particular regard to self driving cars' (2017) Diritto Mercato Technologia, <https://www.academia.edu/35993304/The_issue_of_data_protection_in_the_Internet_of_Things_with_particular_regard_to_self_diving_cars_2017_DIMT> accessed 09 December 2019
- Guarnizo, Juan and Pawel Szalachowski, 'PDFS: Practical Data Feed Service for Smart Contracts' (*ESORICS*, 2018). DOI:10.1007/978-3-030-29959-0_37

- IOT Analytics, 'Connected Streetlights 2018-2023' (Market Report, June 2018)
- ITU (International Telecommunication Union), 'The Internet of Things' (*ITU Internet Reports* 2005)
- ITU (International Telecommunication Union), 'Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security' (2018)
- Li, Xin; Hess, Traci J and Valaich, Joseph S, 'Why do we trust new tecchnology? A study of initial trust formation with the organizational information systems' (2008) 17 (1) The Journal of Strategic Information Systems, 39-71
- Madakam, Somayya et al., 'Internet of Things (IoT): A literature overview' (2015) 3 (5) Journal of Computer and Communications, 165-173.
- Maglaras, Leandros A.; Al-Bayatti, Ali H.; He, Ying; Wagner, Isabel and Janick, Helge, 'Social Internet of Vehicles for Smart Cities' (2016) 5 (1) Journal of Sensor and Actuator Networks, doi: 10.3390/jsan5010003
- McKnight, D. Harrison, 'Trust in Information Technology' in G. B. Davis (ed), *The Blackwell Encyclopedia of Management*. Vol. 7 *Management Information Systems* (Blackwell 2005) 329-331
- National Intelligence Council, 'Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests out to 2025' (SRI Consulting Business Intelligence 2008) <https://fas.org/irp/nic/disruptive.pdf> accessed 9 December 2019
- Oram, Andy (ed), *Peer-to-peer: Harnessing the Power of Disruptive Technologies* (1st edn, O'Reilley Media 2001)
- Saravan, A. and Bama, Sathya S., 'A Review on Cyber Security and the Fifth Generation Cyberattacks' (2019) 12 (2) Oriental Journal of Computer Science and Technology 50-56
- Shama, Pradip Kumar; Moon, Seo Yeon and Park, Jong Hyuk, 'BlockVN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City' (2017) 13 (1) Journal of Information Processing Systems, 184-195
- Shrestha, Rakesh; Bajracharya, Rojeena and Nam, Seung Yeob, 'Blockchain-based Message Dissemination in VANET' (2018 IEEE

3rd International Conference on Computing, Communication and Security (ICCCS), 2018) 161-166

Skulimowski, Andrzej M.J.; Sheng, Zhengguo; Khemiri-Kallel, Sondès; Cérin, Christophe and Hsu, Ching-Hsien (eds), *Internet of Vehicles. Technologies and Services Towards Smart City: 5th International Conference*, *IOV 2018, Proceedings* (Springer 2018)

– Somkutas, Péter and Kőhidi, Ákos, 'Az önvezető autó szoftvere magas szintű szellemi alkotás vagy kifinomult károkozó?' (2017) (2) In Medias Res 232-269

– Tian, Huirong, 'Introduction of IOV Security' *Security Research Institute, CAICT, 2017-11-02*

– Todd, Adam, 'Using a Human Rights Framework for Regulating the Internet of Things: The Critical Role of Human Rights Advocacy' (Conference: The Social Practice of Human Rights, 2019) <https://ecommons.udayton.edu/human_rights/2019/events/61> accessed 9 December 2019

– Tzafestas, Spyros G, 'Ethics and Law in the Internet of Things World' (2018) 1 Smart Cities, 98-120

– UN-GGIM, *Future Trends in geospatial information management: the five to ten year vision* (2nd edn, August 2015)

– Voshmgir, Shermin, *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy* (BlockchainHub 2019)

– Waldman, Mark; Cranor, Lorrie Faith and Rubin, Avi, 'Trust' in Oram, Andy (ed), *Peer-to-peer: Harnessing the Power of Disruptive Technologies* (1st edn, O'Reilley Media 2001) 153-170

– Wang, You-Chiun and Chen, Guan-Wei, 'Efficient Data Gathering and Estimation for Metropolitan Air Quality Monitoring by Using Vehicular Sensor Networks' (2017) 66 (8) IEEE Transactions on Vehicular Technology, 7234-7248. DOI: 10.1109/TVT.2017.2655084

– Weber, Mark; Domeniconi, Giacomo; Chen, Jie; Weidele, Daniel Karl I.; Bellei, Claudio; Robinson, Tom and Leiserson, Charles E., 'Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics' in *Proceedings of ACM Conference* (KDD '19 Workshop on Anomaly Detection in Finance) (ACM 2019)

– Williams, Stephen P., *Blockchain: The Next Everything* (Scribner 2019)

- World Bank Group, 'Internet of Things. The New Government to Business Platform' (Working Paper, 2017)
- World Economic Forum, *The Global Information Technology Report 2015* (2015) ICTs for Inclusive Growth
- Yang, Fangchun; Wang, Shangguang; Li, Jinglin; Liu, Zhinan and Sun, Qibo, 'An Overview of Internet of Vehicles' (2014) 11 (10) China Communications, 1-15

Short biography of the author

Mrs *Judit Glavanis PhD* is associate professor and head of department at Széchenyi István University Faculty of Law and Political Sciences Department of International and European Law. Her main research areas are private international law, in particular international trade law and international financial law. As a public procurement specialist her interest is both theoretical and empirical, focusing on the innovation in financial contracts and services, with special interest in smart contracts and the possibilities of the use of blockchain technology in public services. She is member of the Hungarian Artificial Intelligence Coalition. With her colleagues in Győr and Budapest they have established the SmartLaw Research Group in 2018, which aims to deal with the legal issues of modern technologies.

Autonomous vehicles – Challenges for EU private international law

Balázs Horváthy*

Abstract: Even though the scholarly literature on autonomous vehicles has placed less emphasis on the private international law aspects, in the recent years the scholarship is showing unquestionably growing interest in this area. This increasing attention is partly a consequence of the more active role the European Union is playing in shaping the policy and legal framework of the new technologies, including the future role of private international law concerning the new technological challenges. Contributing to this narrative, the main question of this paper is, whether the private international law is capable of responding adequately to the challenges posed by the future introduction and spreading of self-driving cars, in other terms, is its current set of rules and its legal dogmatics is able to accommodating and addressing the emerging issues of the technological revolution. The paper is focusing on the existing EU legislation, examines how the conflicts of laws could be resolved, how the current EU law might be working in future, hypothetical situations..

Keywords: Autonomous vehicles, artificial intelligence, private international law, EU law

1. Introduction

It is most likely that the first prediction of fully autonomous and connected cars has been put into words by the celebrated writer of science-fiction literature, *Isaac Asimov* in 'Sally', a novel published in 1953. [1] The main character of the story was an apple green "*2045 convertible with a Hennis-Carleton positronic motor and an Armat chassis*"[2] It is also clear from the very detailed technical description of the

The underlining research of this paper has been conducted within the project ''Legal issues of Autonomous Vehicles'' (project No. GINOP-2.3.4-15-2016-00003 Center for University-Industry Cooperation at Széchenyi University).

* Research fellow (Centre for Social Sciences, Institute for Legal Studies); Associate professor (Széchenyi István University, Deák Ferenc Faculty of Law and Political Sciences, Department of International and European Law). E-mail: horvb@ga.sze.hu.

[1] Isaac Asimov: Sally. *Fantastic*, Vol. 2. No. 3., May – June 1953, 36. Online available at https://archive.org/stream/Fantastic_v02n03_1953-05-06#page/n33/mode/2up.

[2] Asimov op. cit. 38.

novel that in the period of the story, automated vehicles are significant and have already spread worldwide, but are extremely expensive playthings: the novel highlights that autonomous transport means are hundred times more expensive than traditional vehicles, therefore only few can afford to own autonomous cars. As a result, due to high level of expenses, the transport revolution has been taken place mostly in the public transport, and the industry was primarily specialized in the production of autonomous buses, which, as much as possible, have been operated as a kind of demand-based communal transport.[3] [4] Moreover the vehicles featured in the novel were able to communicate with each other, so according to our today's concepts *Asimov* wrote about the 'connected cars'. It is important from the perspective of this study, that one of the most important turning points of the short story has been a criminal offense committed by an autonomous bus, when it caused a road accident and run over a 'human' character killed him 'intentionally'. Moreover, *Asimov* explicitly referred to the law in his novel, when one of his 'human' character admitted: "[...] I remember when the first laws came out forcing the old machines off the highways and limiting travel to automatics. Lord, *what a fuzz*."[5]

Taken *Asimov*'s prophecy out of context, these predictions can be easily associated with the current problems of autonomous vehicles and the revolutionary changes in the automotive industry and transport. In addition, the above examples arising from the science-fiction literature illustrate evidently that the broad social challenges comprise the legal narratives and the legal concerns have to be taken into account as well. The law must reflect on the likely challenges and social developments still in time, it means prior to the technology's introduction which might help

[3] It is easily to see that the vision in this prediction is similar to the current forms of flexible transport services. The demand-responsive transport is already very common form of shared transport services, applied also in certain European countries, where the vehicles, busses, coaches, etc. are circulating not on fix routes, but enables the passengers to signalize in advance that they want to get on, and the vehicles will establish the final route based on these demands.

[4] See Asimov's description: „*You could always call a company and have one stop at your door in a matter of minutes and take you where you wanted to go. Usually, you had to drive with others who were going your way, but what's wrong with that?*" Asimov op. cit. 38.

[5] Asimov op. cit. 38.

to avoid the fuzz – or "fuss" in this context – to which *Asimov* referred in his novel.[6]

In the last few years, the legal scholarship is increasingly focusing on this area, the private law, [7] legal theory and ethics,[8] criminal law,[9] as well

[6] The vision of this "fuss" or "fuzz" could remember us to the descriptions of the technological revolution taken place nowadays, where this process is frequently called 'disruptive'. The new technologies are 'disruptive' in a sense that these are now building entirely new structures in a way that, at the same time, 'disrupt' or even demolish our traditional social structures, our traditional knowledge etc. See: James Manyika – Michael Chui – Jacques Bughin – Richard Dobbs – Peter Bisson – Alex Marrs: Disruptive technologies: *Advances that will transform life, business, and the global economy*. McKinsey Global Institute, New York, 2013. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies (2019.07.15.).

[7] See especially: Kyle Colonna: Autonomous Cars and Tort Liability. *Case Western Reserve Journal of Law, Technology & the Internet*, 2013/4. https://ssrn.com/abstract=2325879 (2019.07.15.); Jan De Bruyne – Jochen Tanghe: Liability for Damage Caused by Autonomous Vehicles: A Belgian Perspective. *Journal of European Tort Law*, 2017/3. 324–371.; Kevin Funkhouser: Paving the Road Ahead: Autonomous Vehicles, Products Liability, and the Need for a New Approach. *Utah Law Review*, 2013/1., 437–462.; Jeffrey K. Gurney: Sue my car not me: products liability and accidents involving autonomous vehicles. *University of Illinois Journal of Law, Technology & Policy*, 2013/2. 247–277.; Maurice Schellekens: Self-driving cars and the chilling effect of liability law. *Computer Law & Security Review*, 2015/4., 506–517.

[8] See Alexander Hevelke – Julian Nida-Rümelin: Responsibility for crashes of autonomous vehicles: an ethical analysis. *Science and Engineering Ethics*, 2015/3., 619–630.; Heather Bradshaw-Martin – Catherine Easton: Autonomous or 'driverless' cars and disability: a legal and ethical analysis. *European Journal of Current Legal Issues*, 2014/3. http://webjcli.org/article/view/344 (2019.07.15.); Joshua Paul Davis: Law Without Mind: AI, Ethics and Jurisprudence. *Univ. of San Francisco Law Research Paper,* No. 2018-05. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=3187513 (2019.07.15.); Tom Michael Gasser: *Grundlegende und spezielle Rechtsfragen für autonome Fahrzeuge*. In: Autonomes Fahren (Hrsg.: Maurer, M. – Gerdes, J. – Lenz, B. – Winner H.), Springer, Berlin – Heidelberg, 2015., 543-574.; Benjamin Sobel: Artificial Intelligence's Fair Use Crisis. *Columbia Journal of Law & the Arts* 2017/1.; Thomas E. Spahn: Is Your Artificial Intelligence Guilty of the Unauthorized Practice of Law? *Richmond Journal of Law & Technology*, 2018/4.

[9] Sabine Gless – Emily Silverman – Thomas Weigend: If Robots cause harm, Who is to blame? Self-driving Cars and Criminal Liability. *New Criminal Law Review: An International and Interdisciplinary Journal*, 2016/3., 412–436; Clint W. Westbrook: The Google made me do it: The complexity of criminal liability in the age of autonomous vehicles. *Michigan State Law Review,* 2017/1., 97–147.

as traffic law[10] are predominantly in centre of attention of the academia. This is not surprising, since the major legal challenges that are already foreseeable, e.g. questions of liability, can be adequately responded within these areas. In addition to these core legal areas, there are however further specific narratives have to be considered as well, including the private international law, the subject of this article. [11] The role of the EU private international law in the area of autonomous driving should not be neglected either, because from a practical point of view, perhaps not so far away, when the autonomous vehicles will start spreading in the roads of the European Union, legal problems related to transport will frequently go beyond the borders between the member states. [12] These cross-border legal problems, e.g. arising from road accidents, will require complex answers. The expected legal problems should be addressed not only by the static perspective of the substantive law (e.g. liability, liability forms, etc.), but also the dynamic aspects will be needed to take into consideration. Putting it differently, not merely the question who is liable is important, but it is also vital, how the substantive law can be made effective, namely, which court in which Member State may act, what is the applicable law or how this court's judgment can be enforced. Questions of this dynamic aspects are to be answered by the private international law.

Even though the literature on autonomous vehicles has placed less emphasis on the private international law aspects, in the recent years the

[10] Konrad Lachmayer: Verkehrsrecht: Rechtsstaatliche Defizite der Regelungen zu Testfahrten. In: Autonomes Fahren und Recht (Hrsg.: I. Eisenberger – Lachmayer – G. Eisenberger), Manz Verlag, Wien, 2017. 147–167. o.

[11] It is probable that after the autonomous cars having spread worldwide, more challenges and questions will arise, far beyond the core issues mentioned above, e.g. like data protection, technical standards, or some borderline questions might arise in traffic law.

[12] The predictions are based on different scenarios. For instance, a prophetic advertisement of Nissan promised in 2013 that the Nissan's first fully autonomous car will be in production and available for customers within 5 years (see Jeffrey R. Zohn: When robots attack: How should the law handle self-driving cars that cause damages. *University of Illinois Journal of Law, Technology & Policy*, 2015/2., 462. o.). Less progressive predictions suggest that fully autonomous vehicles will be on the roads in great strength not earlier than the 2040s. See: Dorothy J. Glancy: Autonomous and Automated and Connected Cars – Oh My! First generation autonomous cars in the legal ecosystem. *Minnesota Journal of Law, Science & Technology*, 2015/2. 622–629.

scholarship is showing unquestionably growing interest in this area. This increasing attention is partly a consequence of the more active role the European Union is playing in shaping the policy and legal framework of the new technologies, including the future role of private international law concerning the new technological challenges. The European Parliament has also commissioned a research paper in order to see what problems might arise in this area due to technological changes taken place in the transportation. [13] As a consequence, although the private international law is still a secondary research area in light of autonomous driving, but the first results and publications are already at hand this time. [14]

Contributing to this narrative, the main question, the current paper is seeking for, is whether the private international law is capable of responding adequately to the challenges posed by the future introduction and spreading of self-driving cars, in other terms, is its current set of rules and its legal dogmatics is able to accommodating and addressing the emerging issues of the technological revolution. However, there are two limitations to the analysis. On the one hand, the following paper offers a "Europe-centric" analysis, i.e. it examines the above objectives from the perspective of private international law of the European Union and consequently considers the cross-border legal relationships within the European Union as a model. On the other hand, this study does not want to join the discussion of the 'narratives', i.e. the debate on how the new technologies could be handled and regarded analogically in our traditional terms. As we will see these debates are of fundamental importance primarily in the area of the substantive law and are therefore not specifically related to the interpretation of EU private international law rules.[15]

[13] Thomas Kadaner Graziano: *Cross-border Traffic Accidents in the EU – the Potential Impact of Driverless Cars.* European Parliament – Directorate-General for Internal Policies of the Union, Brussels, 2016. http://www.europarl.europa.eu/thinktank/hu/document.html?reference=IPOL_STU%282016%29571362 (2019.07.15.).

[14] Jan De Bruynen – Cedric Vanleenhove: The Rise of Self-Driving Cars: Is the Private International Law Framework for non-contractual obligations posing a bump in the road? IALS Student Law Review, 2018/1., 14–26. o.

[15] This means that we are not attempting to determine whether autonomous vehicles, as objects of legislation, can be approached *per analogiam* within the current conceptual basis of the legislation governing other types automated vehicles (e.g. automated trains etc.), or we need completely unique law, as the autonomous cars might be *sui generis* phenomenon.

Consequently, the present study is focusing on the existing EU legislation, examines how the conflicts of laws could be resolved, how the current EU law might be working in hypothetical situations. In the analysis we use a hypothetically constructed model case that helps us to demonstrate how particular provisions of the EU law could address questions that might arise in traffic road accidents in the (possibly not too far) future. The next chapter explains this model case and clarifies some basic concepts (*2. Autonomous vehicles and private international law*), then it examines the jurisdiction (*3. The main problems of jurisdiction*), the applicable law (*4. Problems of the applicable law*) and finally closes with a conclusion (*5. Concluding remark*s).

2. Autonomous vehicles and private international law

Although the study does not aim at giving a detailed analysis of the technological background of autonomous vehicles, it is essential to clarify the underlying basic concepts. The popular media uses for 'autonomous vehicles' a couple of terms (self-driving cars, driverless vehicles, automated vehicles, etc.), which are often misplaced or used wrongly as synonyms, or are referring to technologies, where the term is inaccurate. The broadest category accepted in the literature is "*automated vehicles*", which include certain kind of vehicles (cars, buses, trucks, etc.) equipped with special, computer controlled technological features that are able to assist the driver: developed forms of these technologies could take over some of the driving functions or even the entire driving process from the driver. Some of these technologies are already in serial production and are available in new cars (e.g. adaptive headlights, frontal collision warning; automatic emergency braking; adaptive cruise control; park assist systems; lane-departure control; or lane-keep assist, etc.), but the broad term covers also the fully driverless cars, in which all driving functions are automated and operated by computers. Strictly speaking, however, only the latter could be considered as an 'autonomous car.' Consequently, the concept of 'automated vehicles' are the broader term that embraces several technological levels of automation, including the 'autonomous vehicles' as a form of the highest level of automation.

The fully autonomous cars are still in test phase but are already operating in traffic in few places – mostly in the US – within a strict and exceptional legal environment. It is, however only a matter of time before

driverless cars are allowed without any exception into traffic. It is expected, that after the introduction of autonomous vehicles, the full technological change will not take place immediately, and autonomous vehicles will co-exist with vehicles at different levels of automation.[16] The law must be prepared also for this initial period, when different technologies will be in operation on the roads at the same time, specifically, private international law must also be able to deal with more complex problems arising from cross-border traffic disputes during this transitional period. This complexity can be easily seen in the below hypothetical, model case for a cross-border traffic accident. The analysis of this paper is fundamentally based on this model case, we will turn back frequently to this case with the intention of illustration and to show, how the EU law provisions could operate in complex, hypothetical situations. The merits of this model case are as follows:

Two cars (Car-1 and Car-2) are involved in a road accident. Car-1 is a conventional vehicle registered in Austria, owned and operated by an Austrian resident and insured by an Austrian insurance company. Car-2 is an autonomous vehicle, owned by a German company that put it into use for its Hungarian employee who operates the car. Car-2 is registered in Germany and insured by German insurance company. The unfortunate accident occurs in Slovakia due to a malfunction of the Li-DAR system of Car-2. Car-2 is marketed by a French company and was manufactured at the site of a Belgian subsidiary of that company. The automaker buys the LiDAR system from a Finnish supplier and its software has been developed by an Irish company.

Considering the facts of the case it is clear that private international law has to answer two fundamental questions. On the one hand, the question arises as to where the participants in the case can bring proceedings to enforce their claim, in other words, which state will have jurisdiction in these proceedings and which forum will decide the dispute? Another important question is what law should be applied by the forum of the procedure. [17]

[16] But this technological coexistence is not exceptional, as even today, 'traditional' cars are operating with cars partially equipped with automated functions. In the categorization of SAE (Society of Automotive Engineers), the fully autonomous cars are at the highest, fifth level of automation, see Glancy op. cit. 631.

[17] International civil procedural law issues may also arise, namely how these judgments can be enforced. This study focuses on the classic issues of private international law, so this aspect is not discussed here.

As the case is a complex of cross-border legal relationships, it is of great importance that which connecting factors, such as the place of residence, the place where the damage occurred, the place where the vehicle is registered, etc., are applied. Below, we examine these main issues from the perspective of EU private international law.

3. The main problems of jurisdiction

3.1. Unification of private international laws in the European Union

The unification of provisions of jurisdictions in the European Union is not a recent process. Even at the very outset of the European integration, the common market made it necessary for the Member States to introduce and apply uniform rules in certain areas of private international law, rather than domestic, national rules based on different approaches and models. Unification eliminated conflicts arising from different national rules, thereby the major objective of this process was to increase the predictability of the application and enforcement of private international law provisions. This was also expected to strengthen the confidence of businesses and other entities operating within the Community in the single market, to generate and increase in the cross-border transactions and ultimately to deepen the common market. This resulted in conclusion of the Brussels Convention in 1968, which introduced uniform rules on jurisdiction and the enforcement of judgments. [18] Later, the amendments of Treaty of Amsterdam made it possible for Member States to replace the Brussels Convention with secondary EU law, and ss a consequence, the "Brussels I" regulation has been adopted in 2001 (Council Regulation (EC) No 44/2001). [19]

In a 2009 report it was indicated the revision of the regulation has been needed, therefore, the Brussels I Regulation was replaced by the

[18] 1968 Brussels Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial mattersBrüsszelben. Consolidated version: OJ C 27. (1998.1.26.), 1. o.

[19] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matter. OJ L 12. (2001.1.16.), 1. o.

Regulation (EU) No 1215/2012 of the European Parliament and of the Council ("Brussels I bis" Regulation). [20]

3.2. The jurisdiction according to the "Brussels I bis" Regulation

The first major question regarding the "Brussels I bis" Regulation is whether the Regulation might apply to disputes relating to autonomous vehicles, namely, in a complex dispute as it has been indicated in the above model case. The scope of the Brussels I bis Regulation is broadly defined, according to which its rules shall apply in civil and commercial matters whatever the nature of the court or tribunal, [21] with only a few specific exceptions. [22] Therefore the scope of the regulation has been defined broadly and neutrally, which means that its applicability is not restricted by technological concern, not even if the subject of the underlying dispute would be road accident involving autonomous vehicles.

The Brussels I bis Regulation lays down general and special rules on jurisdiction that all serve the predictability. Moreover, three other major concerns are also shaping the logic and characteristics of the Regulation.[23] First, it designates the defendant's domicile (*locus domicilii*)

[20] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[21] Brussels I bis, Article 1 para. 1.

[22] See Brussels I bis, Article 1 para. 1–2 It shall not extend, in particular, to revenue, customs or administrative matters or to the liability of the State for acts and omissions in the exercise of State authority (*acta iure imperii*), and the the regulation shall not apply to 1. the status or legal capacity of natural persons, rights in property arising out of a matrimonial relationship or out of a relationship deemed by the law applicable to such relationship to have comparable effects to marriage; 2. bankruptcy, proceedings relating to the winding-up of insolvent companies or other legal persons, judicial arrangements, compositions and analogous proceedings; 3. social security; 4. arbitration; 5. maintenance obligations arising from a family relationship, parentage, marriage or affinity; 6. wills and succession, including maintenance obligations arising by reason of death..

[23] Xandra Kramer – Alina Ontanu – Michiel de Rooij – Erlis Themeli – Kyra Hanemaayer: The application of Brussels I (Recast) in the legal practice of EU Member States. Synthesis Report. Asser Institute, Den Haag, 2018. 5. o. https://www.asser.nl/media/5018/m-5797-ec-justice-the-application-of-brussels-1-09-outputs-synthesis-report.pdf (2019.07.15.).

as a general rule of jurisdiction, following the principle of *actor sequitur forum rei*, which prevents the defendant from being sued before a foreign court to which the party has not got any real connection.[24] Second, derogating from the general rules of jurisdiction, the Regulation also establishes specific rules of jurisdiction for cases in which the except can be justified by the interests of the weaker, more vulnerable party (e.g. consumer, insured person, employee, etc.). Third, the regulation also respects the parties' autonomy and allows for forum choice (*prorogatio fori*), provided that it does not violate the criteria indicated in specific jurisdiction cases. For the purpose of the model case, the following rules of jurisdiction are practically important:

a) Under the general rule of jurisdiction, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State. [25] It is also important, that persons who are not nationals of the Member State in which they are domiciled shall be governed by the rules of jurisdiction applicable to nationals of that Member State. .[26] This rule governs also the status of legal person: according to the specific provision of the Regulation, a company or other legal person or association of natural or legal persons is domiciled at the place where it has its statutory seat, central administration, or principal place of business. [27] Consequently, under the general rule of jurisdiction, the defendant may cover all possible persons involved in a traffic accident, as it was indicated in the above model case, i.e. the general rule, the *locus domicilii* may be relevant for a driver, operator, manufacturer, distributor, software developer, etc. of a car, when the court wants to determine its jurisdiction.

b) The regulation lays down special provisions for jurisdiction, which covers also the delicts. As a consequence, a person domiciled in a Member State may be sued in another Member State in matters relating

[24] Mádl Ferenc – Vékás Lajos: Nemzetközi magánjog és nemzetközi gazdasági kapcsolatok joga. Eötvös Kiadó, Budapest, 2014. 305. o. https://www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_527_nemzetkozi_maganjog (2019.07.15.).

[25] See Brussels I bis Article 4 para. 1.

[26] Brussels I bis Article 4 para. 2.

[27] Brussels I bis Article 63 para. 1.

to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur.[28]

c) The special jurisdiction preserved for the so called 'adhesive procedures' might have relevance also in disputes arising from road accidents, in which autonomous vehicles are involved, According to this special rule, a person domiciled in a Member State may be sued in another Member State as regards a civil claim for damages or restitution which is based on an act giving rise to criminal proceedings, in the court seised of those proceedings, to the extent that that court has jurisdiction under its own law to entertain civil proceedings.[29]

d) The regulation lays down special rules for jurisdiction in matters relating to insurance. According to that, an insurer domiciled in a Member State may be sued in the courts of the Member State in which he is domiciled (*locus domicilii*). It is also possible to bring the case to an another Member State, if the actions brought by the policyholder, the insured or a beneficiary. In this case the jurisdiction of the courts is determined by the place where the claimant is domiciled (*locus actoris*). Even though the previous listing does not mention explicitly, according to the case law of the CJEU it includes the injured party as well. Special rules apply for cases where co-insurer has also interest: the co-insurer can bring the case to the courts of a Member State in which proceedings are brought against the leading insurer.[30]

In addition to the previous special jurisdictions, in respect of liability insurance or insurance of immovable property, the insurer may be sued in the courts for the place where the harmful event occurred (*locus damni*). The same applies if movable and immovable property are covered by the same insurance policy and both are adversely affected by the same contingency.[31] In respect of liability insurance, the insurer may also, if the law of the court permits it, be joined in proceedings which the injured party has brought against the insured.[32]

[28] Brussels I bis Article 7 para. 2.

[29] Brussels I bis Article 7 para. 3.

[30] Brussels I bis Article 11 para. 1.

[31] Brussels I bis Article 12.

[32] Brussels I bis Article 13. The specific directive on civil liability allows explicitely to take action directly to the insurer, see Directive 2009/103/EC of the European

The 'protecting the weaker party' principle is also represented in the special jurisdiction provisions of the regulation. Therefore an insurer may bring proceedings only in the courts of the Member State in which the defendant is domiciled, irrespective of whether he is the policyholder, the insured or a beneficiary. [33] Logically, this provisions does not imply the counter claims, i.e. a counter-claim can be brought in the court in which the original claim is pending. Moreover, the parties may depart from this principle by an agreement, but only within strict circumstances.[34]

4.4. Problems of the applicable law

4.1. EU and international unifications regarding the applicable law

Similar considerations we have seen *vis-a-vis* the jurisdiction, Member States harmonized their national rules. In other terms the proper functioning of the common market, the predictability of the settlement of disputes and legal certainty required that the applicable law should be determined in the same way, regardless of the fact, in which the Member State the action has been taken. In the absence of harmonized rules, however, the choice of forum could influence, which substantive law will decide the dispute, therefore it could even influence the outcome of the dispute (*forum shopping*). The unification at Community level, in comparison with the Brussels Convention, started later in this area. After a longer period of preparation, the Convention on the law applicable to

Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability, Article 18. OJ L 263 11 (2009.7.10.).

[33] Brussels I bis Article 14 para. 1

[34] See Brussels I bis Article 15, agreements 1. which is entered into after the dispute has arisen; which allows the policyholder, the insured or a beneficiary to bring proceedings in courts other than those indicated in this Section; which is concluded between a policyholder and an insurer, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, and which has the effect of conferring jurisdiction on the courts of that Member State even if the harmful event were to occur abroad, provided that such an agreement is not contrary to the law of that Member State; which is concluded with a policyholder who is not domiciled in a Member State, except in so far as the insurance is compulsory or relates to immovable property in a Member State; or which relates to a contract of insurance in so far as it covers one or more of the risks set out in the regulation.

contractual obligations (Rome Convention) was adopted in 1980[35] and has been replaced by a regulation later (the "Rome I Regulation").[36]

However, with regard to the non-contractual obligations directly related to our subject, the unification has arrived only in 2007 by the adoption of Parliament and Council Regulation (EC) No 864/2007 ("Rome II").[37] It is important however, that, there are also international agreements in this area, which are relevant, as certain EU Member States have concluded agreements prior to the adoption of the Rome II Regulation. The Regulation itself lays down its relationship to these international conventions, which may be a special norm and take precedence, [38] i.e. the applicable law should be determined not by the Rome II Regulation but by the international convention. Two Conventions are relevant to our analysis: Convention of 4 May 1971 on the Law Applicable to Traffic Accidents[39] and the Hague Convention of 2 October 1973 on the Law Applicable to Products Liability. [40] Many EU Member States are parties of both Conventions, but Hungary takes not part in these conventions. [41] It means that there is a parallel system in the

[35] Rome Convention on the Law Applicable to Contractual Relations, HL L 266 (1980. 10.9.). 1. o.

[36] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations.

[37] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199, 31.7.2007, p. 40–49.

[38] According to that, the regulation shall not prejudice the application of international conventions to which one or more Member States are parties at the time when the regulation has been adopted and which lay down conflict-of-law rules relating to non-contractual obligations. See Article 28. For the parallel regimes, see: Nagy Csongor Istvan: The Rome II Regulation and Traffic Accidents: Uniform Conflict Rules with Some Room for Forum Shopping – How So? *Journal of Private International Law*, 2010/1. 93–108.; Thomas Kadner Graziano: The Rome II Regulation and the Hague Conventions on Traffic Accidents and Product Liability – Interaction, conflicts and future perspectives. *Nederlands Internationaal Privaatrecht*, 2008, 425–429.

[39] Hague Convention of 4 May 1971 on the law applicable to traffic accidents. https://www.hcch.net/en/instruments/conventions/full-text/?cid=81. (2019.07.15.).

[40] Hague Convention of 1 October 1973 on the Law Applicable to Products Liability. https://www.hcch.net/en/instruments/conventions/full-text/?cid=84. (2019.07.15.).

[41] The 1971 Hague Convention has actually 21 contracting parties, which include 13 EU member states (Ausztria, Belgium, Czech Republic, France, Netherlands, Croatia, Poland, Latvia, Lituania, Luxemburg, Spain, Slovakia and Slovenia (Portugalia signed, but not ratified the convention), see:

European Union for the applicable law to non-contractual obligations, [42] thus in addition to the rules of the Rome II Convention, the Hague Conventions are discussed below.

4.2. The Rome II regulation

The first substantive question in the context of the Rome II Regulation is whether it applies to damage caused by autonomous vehicles in road accidents. It sets out the scope of the Regulation in a neutral and universal manner. Aside from certain exceptions, [43] the scope of the Regulation is to apply to non-contractual obligations in the field of civil and commercial matters. The nature of non-contractual obligations is also broadly interpreted in the Regulation, so that damages include all consequences of wrongful harm, unjust enrichment, unlicensed

https://www.hcch.net/en/instruments/conventions/status-table/?cid=81). The parties of the 1973 Hague Convention are 11, in which there are 7 EU member states: Finnland, France, Netherlands, Croatia, Luxemburg, Spain, Slovenia (Belgium, Italy and Portugal have been signed, but not ratified the convention), see: https://www.hcch.net/en/instruments/conventions/status-table/?cid=84).

[42] See: Nagy Csongor Istvan: The Rome II Regulation and Traffic Accidents: Uniform Conflict Rules with Some Room for Forum Shopping – How So? *Journal of Private International Law*, 2010/1. 93–108.

[43] From the scope of the regulation are excluded: non-contractual obligations arising out of family relationships and relationships deemed by the law applicable to such relationships to have comparable effects including maintenance obligations; non-contractual obligations arising out of matrimonial property regimes, property regimes of relationships deemed by the law applicable to such relationships to have comparable effects to marriage, and wills and succession; non-contractual obligations arising under bills of exchange, cheques and promissory notes and other negotiable instruments to the extent that the obligations under such other negotiable instruments arise out of their negotiable character; non-contractual obligations arising out of the law of companies and other bodies corporate or unincorporated regarding matters such as the creation, by registration or otherwise, legal capacity, internal organisation or winding-up of companies and other bodies corporate or unincorporated, the personal liability of officers and members as such for the obligations of the company or body and the personal liability of auditors to a company or to its members in the statutory audits of accounting documents; non-contractual obligations arising out of the relations between the settlors, trustees and beneficiaries of a trust created voluntarily; non-contractual obligations arising out of nuclear damage; non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation. See Rome II regulation Article 1.

administration or *culpa in contrahendo*, as well as all types of damage that is likely to occur. [44] Similarly to the Brussels I bis Regulation, the scope is defined in a neutral manner, i.e. it does not require any special prerequisites, e.g. technological, technical requirements related to damages, therefore the Rome II Regulation also seems to be applicable in disputes arising from road accidents. In addition, it is important that the approach of the Rome II Regulation is universal, it menas that it applies even if the connecting factor refers to the law of a third country, outside the European Union. [45]

The connecting factors determining the applicable law are defined in several ways in private international law. The most common approach that the connecting factors are determined by the characteristics, specificities of the case (e.g. *lex loci delicti commissi, lex loci damni*, etc.). Moreover, the connecting factors can be defined on the basis of abstract, generic concepts (e.g. closest relation principle). The Rome II Regulation combines these methods and provides a flexible framework for conflict-of-law rules. In doing so, the regulation ensures that the applicable law is determined in the most appropriate way and it is not only legally but also predictably fair to the parties of the dispute. For the non-contractual obligations, it is particularly important that the determination of the applicable law should reflect on a balance between the interests of the injured party and those who caused the damage. Considering these aspects, the Rome II Regulation designates the applicable law in the areas relevant to our subject matter in the following manner:

a) Respecting the autonomy of the parties, the Rome II Regulation allows the parties themselves to choose the applicable law to a non-contractual obligation (freedom of choice).[46] The choice of law must be expressly formulated, and must not prejudice the rights of third parties. The choice of law may take the form of an agreement following the occurrence of the event giving rise to the injury or, if all parties are engaged in commercial activities, of an agreement freely negotiated prior to the occurrence of the event giving rise to the damage. Obviously, the

[44] Rome II regulation Article 1 Para. 1–3.
[45] Cf. Rome II regulation Article 3.
[46] Rome II regulation Article 14.

choice of law cannot be derogated from the cogent or imperative rules of the applicable law. [47]

b) In the absence of choice of law, the regulation applies the *lex loci damni* as a general rule, irrespective of the country or countries in which the indirect consequences of the harmful act may occur. [48] For this reason, e.g. in the case of personal injury or damage in the event of a traffic accident, the State of the *lex loci damni* shall be the place where the injury was sustained or the place where the material damage occurred.[49] Therefore, when applying the main connecting factor, it is irrelevant, where the act was giving rise. In traditional traffic accidents, the *lex loci damni* and the *lex loci commissi delicti* are usually identical, but in more complex legal disputes, the wrongful act (e.g. software update that have been wrongly installed etc.) may differ from the *lex loci damni*, but even in these cases the law of the place where the damage occurred shall apply.

c) If the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply; [50]

d) The Rome II Regulation applies the principle of closer relationship as an additional rule (the so-called "escape clause").[51] Where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated above, the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question.

[47] Rome II regulation Article 14 para. 3–4. Burián László – Ziegler Dezső Tamás – Kecskés László – Vörös Imre: *Európai és magyar nemzetközi kollíziós magánjog*. Krim, Budapest, 2010. 244–245. o.

[48] Rome II regulation Article 4 . cikk para. 1. Ld. Burián – Ziegler – Kecskés – Vörös: op. cit. 247. o.

[49] Therefore the Rome II regulation does not use the traditional *lex loci delicti commissi* connecting factor. See: Mádl – Vékás: op. cit. 234. *Lex loci damni*hoz ld. Burián – Ziegler – Kecskés – Vörös: op. cit. uo.

[50] Rome II regulation Article 4. para. 2.

[51] Rome II regulation Article 4 para. 3.

e) Unlike the general rules, the Rome II Regulation lays down specific conflict-of-law rules for product liability. This may be of particular importance, when the damage arise from use of high technology. In these case the court should determine the applicable law according to these specific rules in the following order:

- first, the law of the country in which the injured party had his habitual residence at the time when the damage occurred, if the product was marketed in that country;
- if no such marketing has taken place, the law of the country in which the product was purchased will apply (provided that the product was marketed in that country);
- or, failing that, the law of the country in which the damage occurred, if the product was marketed in that country.

The above exceptional rules can be applied if the person liable could reasonably foreseeable that the product was marketed in the country of applicable law. Otherwise, the applicable law is the law of the country where the person responsible is habitually resident. The regulation also derogates from these three layers of rules, referring to the closer connection principle, as a partial exception in the area of product liability.

f) The Rome II Regulation also enables the member states to refer to the public order (*ordre public*). On that basis, the judge may refuse to apply the law indicated in the regulation, if it is manifestly incompatible with the public policy of the forum. [52] This provides an exceptional opportunity for the forum, which is in principle free to determine the scope of public order in the Member States, without being subject to any substantive limitation in the Regulation. Such public order/public policy grounds could, for example, might be important, if the applicable law would require, e.g. the application of punitive damages, [53] which would be incompatible with the forum's legal system. [54] In these cases, the forum's own law (*lex fori*) will prevail over the law as defined above.

IV. Conclusion

[52] Rome II regulation Article 26.

[53] See Burián – Ziegler – Kecskés – Vörös o p. cit. op. cit. 259. o.

[54] The preamble of the regulation refers to some example, e.g. non-compensatory exemplary or punitive damages, Rome II regulation, preamble 32.

The above analysis has shown that the framework of current EU private international law rules might address the problems of cross-border disputes arising from traffic accidents caused by autonomous vehicles. However, it would be an exaggeration to say that the under the current legislation would be entirely appropriate and needs neither far-reaching reform nor small correction. Actually neither the Brussels I bis nor the Rome II Regulations contain specific provisions for road accidents. Both EU regulations aim to strike a balance between the interests of the litigants – plaintiff and defendant, injured and injured, etc. –, so that both rules of jurisdiction and the applicable law are incorporated in a balanced system. The 'equilibrium' can still be maintained on the basis of the current EU law provisions of non-contractual liability, however, when the autonomous vehicles started spreading across Europe, the nature of road accidents will change, and the period when conventional vehicles and fully autonomous vehicles are involved in transport will be a particular challenge for the EU legislator. Consequently, while in a typical road accident today, the negligence or intentional act of the persons concerned (e.g. not keeping the speed limits, etc.) plays a much larger role than objective factors such as technical reasons, technical problems, etc., this situation will change significantly with the arrival of autonomous vehicles. Just as the "human" drivers bound to their own decisions will be replaced by the "robot drivers" based on artificial intelligence, the causes of road accidents will change. As a result, the current balance between the interests of those involved in a road accident is also shifting, which means that victims (passengers, pedestrians, etc.) must receive considerably more attention. Changes in the nature of road accidents and the objective liability indicated above may also lead to an increase in the proportion of product liability claims and related litigation. Compared to the concept of non-contractual damages, the rules of jurisdiction and conflict of laws regarding product liability are already closer to the model that focuses on the injured party, however, the specificities of possible product liability claims related to autonomous vehicles and artificial intelligence should also be investigated. As we have also seen, the applicable law is determined currently by two coexisting, parallel regimes, i.e. the Rome II Regulation and the Hague Conventions. The coexistence of these regimes is already giving rise to the *forum shopping*, which obviously poses the risk that the parties could not enforce their claims effectively. For this reason, this 'double-regime' also endangers the predictability, which is

fundamental concern in the EU private international law. As a result, it is suggested to review *de lege ferenda* the relation of the Rome II Regulation to other international agreements, specifically to the Hague Conventions.

References

- Heather Bradshaw-Martin – Catherine Easton: Autonomous or 'driverless' cars and disability: a legal and ethical analysis. European Journal of Current Legal Issues, 2014/3. http://webjcli.org/article/view/344 (2019.07.15.)
- Burián László – Ziegler Dezső Tamás – Kecskés László – Vörös Imre: Európai és magyar nemzetközi kollíziós magánjog. Krim, Budapest, 2010.
- Kyle Colonna: Autonomous Cars and Tort Liability. Case Western Reserve Journal of Law, Technology & the Internet, 2013/4. https://ssrn.com/abstract=2325879 (2019.07.15.)
- Jan De Bruynen – Jochen Tanghe: Liability for Damage Caused by Autonomous Vehicles: A Belgian Perspective. Journal of European Tort Law, 2017/3. 324–371.
- Jan De Bruynen – Cedric Vanleenhove: The Rise of Self-Driving Cars: Is the Private International Law Framework for non-contractual obligations posing a bump in the road? IALS Student Law Review, 2018/1., 14–26. o.
- Joshua Paul Davis: Law Without Mind: AI, Ethics and Jurisprudence. Univ. of San Francisco Law Research Paper, No. 2018-05. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=3187513 (2019.07.15.)
- Kevin Funkhouser: Paving the Road Ahead: Autonomous Vehicles, Products Liability, and the Need for a New Approach. Utah Law Review, 2013/1., 437–462. o.
- Tom Michael Gasser: Grundlegende und spezielle Rechtsfragen für autonome Fahrzeuge. In: Autonomes Fahren (Hrsg.: Maurer, M. – Gerdes, J. – Lenz, B. – Winner H.), Springer, Berlin – Heidelberg, 2015., 543–574. o.
- Dorothy J. Glancy: Autonomous and Automated and Connected Cars – Oh My! First generation autonomous cars in the legal

ecosystem. Minnesota Journal of Law, Science & Technology, 2015/2. 622–629. o.
– Sabine Gless – Emily Silverman – Thomas Weigend: If Robots cause harm, Who is to blame? Self-driving Cars and Criminal Liability. New Criminal Law Review: An International and Interdisciplinary Journal, 2016/3., 412–436. o.
– Jeffrey K. Gurney: Sue my car not me: products liability and accidents involving autonomous vehicles. University of Illinois Journal of Law, Technology & Policy, 2013/2. 247–277. o.
– Alexander Hevelke – Julian Nida-Rümelin: Responsibility for crashes of autonomous vehicles: an ethical analysis. Science and Engineering Ethics, 2015/3., 619–630. o.
– Thomas Kadner Graziano: The Rome II Regulation and the Hague Conventions on Traffic Accidents and Product Liability – Interaction, conflicts and future perspectives. Nederlands Internationaal Privaatrecht, 2008, 425–429. o.
– Thomas Kadaner Graziano: Cross-border Traffic Accidents in the EU – the Potential Impact of Driverless Cars. European Parliament – Directorate-General for Internal Policies of the Union, Brussels, 2016. http://www.europarl.europa.eu/thinktank/hu/document.html?reference=IPOL_STU%282016%29571362 (2019.07.15.)
– Xandra Kramer – Alina Ontanu – Michiel de Rooij – Erlis Themeli – Kyra Hanemaayer: The application of Brussels I (Recast) in the legal practice of EU Member States. Synthesis Report. Asser Institute, Den Haag, 2018. https://www.asser.nl/media/5018/m-5797-ec-justice-the-application-of-brussels-1-09-outputs-synthesis-report.pdf (2019.07.15.)
– Konrad Lachmayer: Verkehrsrecht: Rechtsstaatliche Defizite der Regelungen zu Testfahrten. In: Autonomes Fahren und Recht (Hrsg.: I. Eisenberger – Lachmayer – G. Eisenberger), Manz Verlag, Wien, 2017. 147–167. o.
– Mádl Ferenc – Vékás Lajos: Nemzetközi magánjog és nemzetközi gazdasági kapcsolatok joga. Eötvös Kiadó, Budapest, 2014. https://www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_527_nemzetkozi_maganjog (2019.07.15.)
– James Manyika – Michael Chui – Jacques Bughin – Richard Dobbs – Peter Bisson – Alex Marrs: Disruptive technologies: Advances

that will transform life, business, and the global economy. McKinsey Global Institute, New York, 2013. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies (2019.07.15.)

- Nagy Csongor Istvan: The Rome II Regulation and Traffic Accidents: Uniform Conflict Rules with Some Room for Forum Shopping – How So? Journal of Private International Law, 2010/1. 93–108. o.
- Maurice Schellekens: Self-driving cars and the chilling effect of liability law. Computer Law & Security Review, 2015/4., 506–517. o.
- Benjamin Sobel: Artificial Intelligence's Fair Use Crisis. Columbia Journal of Law & the Arts 2017/1.
- Thomas E. Spahn: Is Your Artificial Intelligence Guilty of the Unauthorized Practice of Law? Richmond Journal of Law & Technology, 2018/4.
- Clint W. Westbrook: The Google made me do it: The complexity of criminal liability in the age of autonomous vehicles. Michigan State Law Review, 2017/1., 97–147. o.
- Jeffrey R. Zohn: When robots attack: How should the law handle self-driving cars that cause damages. University of Illinois Journal of Law, Technology & Policy, 2015/2.
- Ződi Zsolt: Platformok, robotok és a jog: Új szabályozási kihívások az információs társadalomban. Gondolat, Budapest, 2018., 217. o.

Short biography of the author

Balázs Horváthy (PhD) is research fellow at the Hungarian Academy of Sciences CSS Institute for Legal Studies (Hungary, Budapest) and associate professor at Szechenyi Istvan University, Faculty of Law and Political Sciences, Department of International and European Law (Hungary, Győr). He obtained his PhD from ELTE University (Hungary, Budapest) in protective measures of the Common Commercial Policy in 2009. He teaches courses in EU public law and policies of the EU, international trade law; and his current research interests include social policy conflicts of EU and international trade law, 'Trade and Environment' issues. He participates in the 'Lendület-HPOPs' Research Group of the Hungarian Academy of Sciences on 'The Policy Opportunities of Hungary

in the EU' between 2013–2019. He has also carried out individual research project on the environmental impacts of international trade law within the Bolyai Research Scholarship of the Hungarian Academy of Sciences (2011–2014). He is a member of the Society of International Economic Law, The University Association for Contemporary European Studies (UACES), Institute for the Danube Region and Central Europe (IDM), and Hungarian Society of International Federation for European Law (FIDE).

Annex

The Centre for European Studies (CES) at the Széchenyi István University

László Milassin*

The Jean Monnet Programme

In 1989, the European Commission launched the Jean Monnet Action to support academic research in European integration. The programme originally addressed academics in the Member States, but came to include those in accession countries soon after. Today, it has a global scope and offers worldwide support to European integration studies.

The most important modes of support have been grants for the development of teaching modules in European integration studies, the designation of Jean Monnet Chairs and financial support for Jean Monnet Centres of Excellence for teaching and research. Networking activities and other research activities are supported too. Cooperation across different institutions and with partners outside higher educations is encouraged.

Grants are a trigger for the development of initiatives, in spite of their modest value and dependency on co-funding. Strong support from the university management is a must because grantees are required to continue activities for a number of years after support has ceased.

Over the years, interdisciplinary has come to grow in importance and is now actively promoted. Indeed, a solid understanding of European integration requires insight from history, politics, economics, law and other disciplines.

The current and former Jean Monnet Chairs form a very strong professional network. Being awarded a Jean Monnet Chair is seen by

* Associate professor (Széchenyi István University, Deák Ferenc Faculty of Law and Political Sciences, Department for International and European Law), and head of the Centre for European Studies (Széchenyi István University, Deák Ferenc Faculty of Law and Political Sciences). E-mail: milassin@sze.hu

many as a valuable entry ticket into the international community of European integration researchers.

European Study Centres in Hungary

In 1998 the Hungarian Representation of the European Commission (DG 10) and the Hungarian Ministry of Foreign Affairs concluded an agreement on establishing 14 European Study Centres with the support of PHARE aid. The European Study Centres were established as parts of 14 Hungarian state accredited universities. Today there are 17 European Study Centres in Hungary. In 2000 the European Study Centres were coordinated by the TEMPUS Public Foundation which elaborated a programme with remarkable results: more than 30.000 undergraduate students, 3.500 graduate students, and 7.000 experts from target group institutions (teachers, entrepreneurs, lawyers, journalists and civil servants) had been trained by more than 600 lecturers.

The main tasks of ESC:

- Teaching of EU modules (EU Law, economic and political integration, history of the European Institutions, etc.) at the faculties on different levels.
- Teaching of European studies in the postgraduate education.
- Training and further educations to experts, businesspersons, officers, attorneys, media specialists and high school teachers.
- Research programs (PhD and other research activities).
- Network building activities (ESC, regional, sectorial and partnership cooperation).

Centre for European Studies at the Széchenyi István University

The European Study Centre of Széchenyi University was established in 1998 too. It focused on the teaching modules which covered the most important knowledge about European integration. The study centre became a real regional centre. Our study centre cooperated very close with the local authorities organizing lectures for civil servants, business professionals and secondary school teachers in the region.

The teaching activities of our centre covered the following subject: case law of the EU, European internal policies, IT law and legislation of the EU, regional politics of the EU, EU project planning, developing the rural

regions in the European Union, European security and defense policy, European transportation infrastructure, EU traffic, tariffs and customs, and development of small regions in the EU. We published a newsletter monthly on European Law.

Since 1998 we have a Jean Monnet Chair at our Faculty of Law. Wee participate actively in the Jean Monnet and ERASMUS+ programmes. Our study centre cooperated and cooperate with the following foreign partner institution: University Vienna Juridicum, University Strasbourg, University Sapientia, University Brno, University Krems, University Jules Verne France, University Passau Germany, University Saarbrücken, etc.

EUBLAW - Jean Monnet Module on EU Business Law (2016-2019)

In 2016 the Centre for European Studies obtained funding for the "Jean Monnet Module on EU Business Law" (EUBLAW) project within the framework of the Erasmus+ programme of the European Union. The main objective of the project concerns comprehensive curriculum development in the field of EU Business Law at the Deák Ferenc Faculty of Law of Széchenyi István University. The project aims at elaborating the scope and content of complex course structure, establishing the methodology of the courses, composing of 2 elective courses announced in English. The new courses will be announced for students attending MA law, for incoming Erasmus-students of the Faculty and also interested students in international administration and economics will have the opportunity to participate. The team members will elaborate up-to-date course materials, including systematised course presentations and a concise course book in English in order to foster the publication and dissemination of the results of academic research conducted within the three years long project. The main aim of the project is to deliver tailor-made courses for the participants and for that reason, the teaching methodology will also apply innovative approaches. The Jean Monnet Module will be predominantly based on the 'law in context' approach and will offer a perspective behind the text of law in order to equip students with the ability to understand the real function of the legal instruments governing the business relations within the EU internal market. In this way, the project is expected to improve teaching capacities in the field of EU Business law in English at the Faculty, as well as to provide quality course materials. The Jean Monnet Module will be carried out within the infrastructure of the Centre for European Studies, therefore the project

might give also new impetus to this research institution of the Faculty established within a former PHARE project in 1998. Moreover, as an expected post-grant impact, the project outcome might contribute to the accreditation of a post-graduate course (LL.M.) for legal professionals as well.