



You have downloaded a document from
RE-BUŚ
repository of the University of Silesia in Katowice

Title: Blockchain and the Law

Author: Dariusz Szostek

Citation style: Szostek Dariusz. (2019). Blockchain and the Law. Baden-Baden: Nomos. DOI: 10.5771/9783845298290



Uznanie autorstwa - Użycie niekomercyjne - Bez utworów zależnych Polska - Licencja ta zezwala na rozpowszechnianie, przedstawianie i wykonywanie utworu jedynie w celach niekomercyjnych oraz pod warunkiem zachowania go w oryginalnej postaci (nie tworzenia utworów zależnych).



UNIwersYTET ŚLĄSKI
W KATOWICACH



Biblioteka
Uniwersytetu Śląskiego




Ministerstwo Nauki
i Szkolnictwa Wyższego

Dariusz Szostek

Blockchain and the Law



Nomos

<https://doi.org/10.5771/9783845298290>, am 17.07.2020, 12:12:27
Open Access -  - <https://www.nomos-elibrary.de/agb>

Dariusz Szostek

Blockchain and the Law



Nomos

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at <http://dnb.d-nb.de>

ISBN 978-3-8487-5693-3 (Print)
978-3-8452-9829-0 (ePDF)

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ISBN 978-3-8487-5693-3 (Print)
978-3-8452-9829-0 (ePDF)

Library of Congress Cataloging-in-Publication Data

Szostek, Dariusz
Blockchain and the Law
Dariusz Szostek
160 p.

ISBN 978-3-8487-5693-3 (Print)
978-3-8452-9829-0 (ePDF)

1st Edition 2019

© Nomos Verlagsgesellschaft, Baden-Baden, Germany 2019. Printed and bound in Germany.

This work is subject to copyright. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage or retrieval system, without prior permission in writing from the publishers. Under § 54 of the German Copyright Law where copies are made for other than private use a fee is payable to "Verwertungsgesellschaft Wort", Munich.

No responsibility for loss caused to any individual or organization acting on or refraining from action as a result of the material in this publication can be accepted by Nomos or the author.

Inhaltsverzeichnis

Introduction	9
Chapter I. Blockchains and DLT in the digital economy	11
Introduction	11
Blockchains – a new digital economy?	17
Introduction	17
Trends of the digital economy	20
DLT and blockchains as a catalyst for lex electronica?	25
Chapter II. Blockchains, DLT – basic terms.	34
DLT – distributed ledgers	34
Definition	34
Legal definition	36
DLT and documents	37
Blockchains	40
Definition	40
Legal definition	42
Blocks	45
Consensus	47
How does it work?	49
Types of blockchains	52
Chapter III. Blockchains in finance	54
Introduction	54
Blockchains in financial institutions	56
Bitcoin and its Bitcoin blockchain	58
Bitcoin – how does its blockchain work?	59
Bitcoin blockchains – legal issues	63
Introduction	63
License for Bitcoin software	64

	Other contracts within the Bitcoin blockchain	71
	Relationships among “miners”	72
	Mining contracts	80
	Relationships among Bitcoin holders	82
	Wallets	82
	Transfers of bitcoins or other cryptocurrencies and blockchain records	85
	Cryptocurrency “exchanges” and buyers	88
	Blockchains or DLT and electronic money	92
Chapter IV.	Durable media with blockchain technology	97
	Introduction	97
	Term of durable medium	97
	Blockchain technology and durable media	102
	Private or public blockchain as technology for durable media?	104
	Use of private blockchains as technology for durable media	104
	Use of public blockchains as technology for durable media	105
	Ways of recording documents on durable media	106
	“Forgetting” a document on a durable medium	108
	“Providing” a document on a blockchain-based durable medium.	108
Chapter V.	“Smart Contracts”	110
	Introduction	110
	Definition of a Smart Contract	112
	From the point of view of the doctrine	112
	Legal point of view	115
	The Notion, Properties and Classification of “Smart Contracts”	116
	Notion and properties	116
	Classification	119

Tokens in “smart contracts”	123
Introduction	123
Definition	125
Tokens – legal issue	127
“Smart contracts” as private law	131
“Smart contracts” and lawyers	131
Custom, common law, lex mercatoria, arbitration and smart contracts	133
Chapter VI. The future of blockchain solutions in legal regulations (an initiated discussion).	136
Appendix	141
Bibliography	153
The Author	159

Introduction

The Internet has been developing, particularly in general business, for a little over twenty years. No previous media developed so fast and none had such great impact on social change, economic development, including development of the so-called digital economy, or on the life of “ordinary people”. The first smartphone, significantly changing the way people behave, as well as access to knowledge, information, data, etc., appeared just 12 years ago. 10 years ago, an unknown creator or group of creators, functioning under the nickname of Satoshi Nakamoto, proposed and launched the blockchain-based smart contract, creating Bitcoin. At first, the concept of blockchain and cryptocurrencies seemed pipe dreams, apparently without any real impact on the economy, as demonstrated by a number of reports (prepared by governments or private institutions) from several years ago. The last 3-4 years have drastically changed that view, both with regard to cryptocurrencies, which are more and more often used or at least tested by financial institutions, including banks, and to the blockchain technology used more and more commonly in numerous areas, such as: power generation, health, education, finance, government, logistics, transportation and others. Many states have made strategic decisions to transfer their resources to blockchain-based systems. In other parts of the world, the first laws regarding blockchains have been adopted. This new technology has resulted in many new fortunes and many entities have been established, but some have also gone bankrupt (including “cryptocurrency exchanges”), and in the meantime the price of one bitcoin skyrocketed to almost USD 20,000 and then dropped to just several thousand. Besides Bitcoin, many other cryptocurrencies were introduced, with a capitalization of several billion dollars.

Therefore, it has become necessary to examine the legal aspects of that technology and its impact not only on the principles and concepts but also on the legal regulations, to define and determine the blockchain-related processes and to standardize the terminology used to describe the technology, as well as to indicate the method for or attempt at solving the problem associated with blockchains in different legal systems. However, the aim of this publication is not to assess blockchain technology or the rationale for introducing it. Its character, just like that of blockchains, is not uniform and refers both to private law and public regulations. Legal issues are inter-

woven with technical ones. The global character of a blockchain and the opportunities related to it have forced a supralocal attitude to that issue, taking into account the cross-border and international character of problems.

A lot of publications, documents and information exist or have been published solely in electronic form, so this study contains many online references.

The research into blockchains has required understanding its essence as well as the IT-related principles of functioning, which forced a number of not only legal, but also technical and IT consultations, within which the easy questions asked to an IT specialist were accompanied by more and more serious questions; cryptocurrencies were tested, including transactions using them, many ICT systems were reviewed and a number of scientific discussions were held with specialists from multiple areas of the law, as well as of cybersecurity, IT, identification, cryptography, ICT systems, etc. I would like to thank them for every discussion and for the time devoted to conversations and online seminars, because without that assistance, neither the scientific research nor this publication would have been possible.

Also, if it had not been for the support from the Universities that provided opportunities for work, internship, scientific research and access to library resources, this publication would not have come to life, especially considering that a number of quoted sources or described legal regulations are just several months old, while others were published while this monograph was being written, and were urgently obtained by partner Universities for the purpose of allowing me to use them and conduct the scientific research.

Opole, 2019

Chapter I. Blockchains and DLT in the digital economy

Introduction

In 2018, one of the most frequent searches in online search engines was “GDPR”. Another one, in which mainly business was interested, was “blockchain”. One year ago, the second most searched phrase in Google¹, in the “global news” category, was the term “Bitcoin” (the interest increased particularly at the end of the year, when Bitcoin reached almost USD 20,000 in bitcoin exchanges). In turn, in the “how to ...” category, the third most searched phrase was “How to buy Bitcoin?”. In numerous conferences, business events, online transmissions, fairs and congresses, these terms are discussed at length, repeated over and over again, the startups dealing with that technology are financed, politicians announce special programs supporting that technology, serious state institutions and international organizations notice it, and a number of reports are prepared.

In February 2018, the European Commission opened the EU Blockchain Observatory and Forum, the purpose of which is to highlight the most important progress in the area of blockchain technology, to support European entities and to intensify the cooperation between the EU and the interested parties operating in that sector. The Commission indicates that “blockchain technology will significantly impact digital services and transform business models in a wide range of areas, such as healthcare, insurance, finance, energy, logistics, intellectual property rights management or government services”. The Commissioner for Digital Economy and Society, Mariya Gabriel, emphasized that venture-capital funds invested over EUR 1.2 billion in over one thousand start-ups in that sector, and the European Commission is projected to provide EUR 340 million until 2020 within the EU research programs Horizon 2020 for the projects making use of blockchain technology. The report prepared for the European Parliament: How Blockchain Technology could change our lives (February 2017) indicates that, in the next several years, that technology will significantly

1 <https://trends.google.pl/trends/explore?date=2017-01-01%202017-12-31&q=Bitcoin> of 11 November 2018.

impact the EU economy² and Europe may not escape from it (Boucher, Nascimento and Kritikos, 2017).

On 10 April 2018, twenty-three European countries (Austria, Belgium, Bulgaria, the Czech Republic, Estonia, Finland, France, Germany, Ireland, Latvia, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and Great Britain) signed the Blockchain Partnership Declaration, which is to be the tool for cooperation among the countries for the purpose of exchanging expertise and experience in the technical and regulatory areas, and preparing blockchain implementations for the whole digital market of the EU, for the benefit of the public and private sectors. The essence of the declaration was mentioned by Mariya Gabriel, Commissioner for Digital Economy and Society: “In the future, all public services will use blockchain technology. Blockchain is a great opportunity for Europe and Member States to rethink their information systems, to promote user trust and the protection of personal data, to help create new business opportunities and to establish new areas of leadership, benefiting citizens, public services and companies. The Partnership launched today enables Member States to work together with the European Commission to turn the enormous potential of blockchain technology into better services for citizens.”³

On 16 May 2018, the Committee on Industry, Research and Energy adopted the draft Resolution for the European Parliament on distributed ledger technologies and blockchains: Building trust with disintermediation (2017/2772(RSP)). It indicated that DLT⁴ (A report by the UK Government Chief Scientific Adviser, 2017) may reinforce the position of citizens who become owners of their data. DLT introduces a paradigm of social value based on information technology which is conducive to autonomy of the person, trust and transparency; requires development of frameworks for legal regulations for the applications based on that technology and may

2 P. Boucher, S. Nascimento, M. Kritikos: How Blockchain Technology could change our lives, Brussels2017, pp. 3 et seq. Source: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA\(2017\)581948_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf) of 9 November 2018.

3 <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership> of 11 July 2018.

4 DLT – Distributed Ledger Technology, more on that term below. See: Distributed Ledger Technology: beyond block chain. (A report by the UK Government Chief Scientific Adviser, 2017), <http://fintechpoland.com/wp-content/uploads/2017/01/Technologie-rozproszonych-rejestrow-UK-GOFS-FTP-NASK-PL-1.pdf> of 11 June 2018.

significantly streamline the operation of key sectors of the economy and improve the quality of government services, providing consumers and citizens with a high level of satisfaction with transactions. It was indicated that DLT may be applied to and significantly impact the financial sector and payment disintermediation, as well as the sectors of energy, health, education and copyrights. The cornerstone of DLT is the so-called “smart contract” – the European Commission is called to test the ISO and CEN_CENELEC technical standards as well as the legal frameworks, with which smart contracts may be legally enforced in the whole uniform market of digital content, instead of fragmented laws in the respective member states⁵.

On 3 October 2018, the European Parliament adopted the resolution on distributed ledgers and blockchain technologies: Building trust with disintermediation (2017/2772(RSP)10), which takes into account the above-mentioned draft resolution of the Committee on Industry, Research and Energy, the resolution of the European Parliament of 26 May on virtual currencies, the resolution of the European Parliament of 28 April on Fin-Tech: the influence of technology on the future of the financial sector, the resolution of 6 February 2018 on geo-blocking and other forms of discrimination based on customers’ nationality, place of residence or place of establishment. The resolution indicated the strategic directions of applying distributed ledger technologies both in the EU and in the member states, among others, the energy sector, ecology (contribution to generation of “green” energy), transportation, healthcare, deliveries, education, copyrights and finance. The European Commission was asked to support the scientific and educational activities related to DLT, and to develop “smart contracts”, to be used, among others, by entrepreneurs. It was also emphasized that blockchains increase the security of technological infrastructure and of the data recorded in it. The European Parliament emphasizes the strategic significance of DLT and blockchains for public infrastructure. The European Commission was asked to develop and implement the strategies aimed at training and reskilling the European community in terms of digital skills. It was also asked quickly to collect the technical knowledge and regulatory capacity in order to be able to undertake quick legislative and regulatory activities. The document presents, in a comprehensive way, the direction for development of the EU and use of a new technology, in a way indicating the strategy for operation in that area for the European Com-

5 http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/RE/2018/05-16/1144650PL.pdf of 11 July 2018.

mission. In the foreseeable future, we should expect further intensive activity of the EU in that scope.

In 2018, Vice President and Prime Minister of the United Arab Emirates Sheikh Mohammed bin Rashid announced the “UAE Blockchain Strategy 2021”, which is to make the United Arab Emirates the global leader in implementing blockchains in 2021. It follows from the estimates made by the government of the United Arab Emirates that almost USD 3 billion is spent annually on document circulation and archiving. It was calculated that replacing traditional documents with electronic ones, based on blockchain technology, in the United Arab Emirates, will save one million hours of work, will allow the number of “produced” documents to decrease by 389 million and limit the number of kilometers of document transportation by 1.6 billion a year. It is expected that in 2021 half of government transactions will be conducted using blockchain technologies⁶.

In the last three years, many serious blockchain consortia and councils have been established in the world, for the purpose of supporting, developing and promoting blockchain technology, as well as its practical application. These councils usually comprise prominent scientists as well as representatives of government organizations and of the biggest global companies from the IT sector. Based on the publication entitled⁷: *Blockchain Consortia and Councils in the World* (Garstka and Piech, 2017), it should be indicated that 252 such councils were identified in 2017. They are mainly registered in the USA, Great Britain, Japan, Canada, China, Luxembourg and Dubai. They were established for, among other purposes, exchange of experience and know-how, and commercialization of blockchain solutions. The opinion-forming arrangements include, among others: World Economic Forum and GFC (26) *The Future of Blockchain* (26 of 35 Global Future Councils), IC3 Initiative for Cryptocurrencies and Contracts in NYC (scientists and leaders of the sector from, among others, Cornell University, Cornell Tech, UC Berkeley and University of Illinois). The arrangements aimed at standardizing blockchains: FCA Sandbox Project, China, ISO TC/307. The most important implementation consortia: Global Blockchain Council – Dubai (government organizations of the United Arab Emirates, but also including Cisco, IBM, SAP, Ericsson and Microsoft), R3CEV Consortium (among others J.P. Morgan, Royal Bank of Scotland, Credit Suisse, Goldman Sachs etc.). The main objective of the

6 <https://comparic.pl/rzad-emiradow-arabskich-chce-stac-sie-swiatowym-liderem-technologiei-blockchain/> of 9 June 2018.

7 Garstka i Piech (2017), pp. 2-20.

consortium is to design and provide advanced blockchain technologies for the global financial markets. Another example is Blockchain Embassy Asia (cooperation between different business entities and Asian society). In June 2016, the consortium of Bank of Canada, Payments Canada and R3 was established in Canada for the purpose of introducing blockchains in the financial infrastructure of Canada. Soon after, the National Bank of Canada, Canadian Imperial Bank of Commerce and ATB Financial enlisted the services of San Francisco-based Ripple Labs to integrate blockchains practically in their business environments⁸.

Also open-source organizations are undertaking activities to promote and implement blockchains. An example is Hyperledger – a community of programmers functioning based on Open-Source principles, managed by the Linux Foundation, which guarantees transparency and openness. The consortium consists of businesses, organizations and individual programmers. The objective of Hyperledger is to develop an open standard developed through architecture frameworks. Within the project, each blockchain initiative should be based on an open standard of protocol and licensing model, and the solution introduced should support communication among various networks based on DLT, blockchains and traditional data systems (System of Record SOR). The developed codes are to provide native support for all types of transactions, regardless of the type of assets (cryptocurrencies, tokens or other values). Therefore, what is necessary is a consensus mechanism, management of roles, administration of network access⁹ etc. (Zandberg-Malec, 2016)

One of the largest blockchain-related joint venture consortia was established in January 2018, consisting of Maersk and IBM, with the following entities interested in the project: General Motors, Procter and Gamble, Agility Logistics, Cypher, DuPont, Dow Chemical, Tetra Pak, Port Houston, Rotterdam Port Community System Portbase, the Customs Administration of the Netherlands, and U.S. Customs and Border Protection. The objective of the consortium is to use blockchains, but also AI and IoT for digital supervision of transfers of goods by, among other methods, tracking

-
- 8 E. Ducas, Al. Wilner: the security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. [in] *International Journal* 2017 No. 72(4) (Ducas i Wilner, *The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada*, 2017) p. 540.
- 9 See M. Jędrzejczyk, Karolina Marzanowicz, *Blockchain jest fundamentem cyfrowej gospodarki opierającej się na współpracy*, ed. J. Zandberg-Malec, [in] *Blockchain, inteligentne kontrakty i DAO*, Warsaw 2016, pp. 26-29 (online publication).

their routes, and also for digital clearance and a paperless approach (excluding paper documents from circulation). Other producers of vehicles are also interested in improvements based on DLT and blockchains. MOBI: Mobility Open Blockchain Initiative was established in May 2018. Its main participants are: BMW, Ford, General Motors and Renault. Other partners include: Accenture, Aioi Nissay Dowa Insurance Services USA, BigChainDB, Dashride, Deon Digital AG, Dovu, Cgronicled, ContextLabs, Crypto Valley Association, Foam, Hyperledger, IBM, IOTA, MotionWerk, NuCypher, Oaken Innovation, Ocean Protocol, ShareRing, Shift, Spherical Analytics, Trusted Internet of Things, Alliance, Vasily, Xain, and ZF Friedrichshafen AG. The objective is to implement blockchain technology in the automotive sector by developing joint standards and API for launching payments and data exchange among vehicles (cars – so also IoT), Ride-sharing and Mobility ecosystem commerce.

Taking the above into consideration, in the world there is visible a serious trend related to blockchain and DLT technologies and their implementation. The engagement of a number of international institutions and organizations, scientists, the largest IT concerns as well as start-ups and single programmers, indicates that it is not only a technological curiosity, and the hundreds of millions of dollars already spent and planned to be spent on that technology demonstrate its very serious economic potential. What is important is that the established consortia are of a supranational, cross-border, or even global, character. They include not only the largest global concerns but also the laboratories and start-ups that develop their technologies based on distributed ledgers. The gigantic financial and organizational support as well as technological resources allow global implementations, the impact of which will be definitely felt also in the local markets. Therefore, it is becoming necessary to analyze DLT and blockchain technologies, but not only from the technical, economic points of view or from the point of view of development of digital technology, as presented in the publications so far, but also from the legal point of view. In other words – how blockchain technology translates and will translate into legal regulations and to what degree will it change the perception of law.

Blockchains – a new digital economy?

Introduction

Before we discuss the technical aspect of blockchains and analyze the legal aspects of implementing them, we should indicate certain areas of application of distributed ledger technologies and the tendencies of their impact on the economy and on legal regulations. It is more and more often indicated that DAO and blockchains constitute the foundations of a new digital economy, significantly separated from domestic economies, concentrating on the global economy. On the one hand, such a statement may seem like a pipe dream, but on the other – there are observable very intense activities aimed at developing a digital economy on different levels, be it global (global concerns), continental (Asia, Europe, America, etc.) or regional¹⁰. (Bartorski, 2012).

At the turn of the 20th century, a number of publications appeared in Europe, the USA and Asia, addressing the phenomenon of the new medium of the Internet. It had an impact on the law at the time and, indirectly, on the economy. There was emphasized the need for a number of changes in the following areas: press law, civil law, intellectual property, Labor law, tax law, criminal law, etc. People asked: to what degree will the Internet impact societies as well as laws and their application? At that time, it was difficult to predict how that medium was going to develop, or even what impact it would have on the economy. The dilemmas and legal issues appearing at that time may seem laughable today, just like the publications from the 1950s and 1960s predicting the impact and legal issues of more and more common use of the phone. Today, similarly, it is difficult to predict the direction of development of blockchain technology, and the current legal problems and dilemmas are often overwhelming not only for individual lawyers but also for serious organizations and institutions. It is probable that in a few years these issues will seem laughable, just like the previous dilemmas related to the Internet.

It is worth emphasizing that, nowadays, we are dealing with a very intense development of the so-called new technologies, on an unprecedented scale. It has to be faced by lawyers, often trying to catch up with the gallop-

10 See also ed. D. Batorski: *Cyfrowa Gospodarka. Kluczowe trendy rewolucji cyfrowej*, Warsaw 2012, p. 3 et seq. http://www.euroreg.uw.edu.pl/dane/web_euroreg_publications_files/1335/cyfrowa_gospodarka_kluczowe_trendy_rewolucji_cyfrowej.pdf of 12 June 2018.

ing pace of change. Twenty years ago, the discussions were related to the spread of desktop computers and data transferred in analog form on durable media, and only later the use of electronic means of communication (Szostek D., *Czynność prawna a środki komunikacji elektronicznej*, 2004)¹¹. At first, the Internet was used solely for short text messages, and the capacity of an email box was usually limited to 20 MB. Online distribution of images, films or sounds was very costly, complicated and, most importantly, slow, and often even impossible. Electronic transmissions and communication became common only later, with the spread of the Internet, fiber-optic connections, development of online portals and stores, and as proper legal regulations followed. However, it needs to be noted that in the first stage, the Internet was mainly used for communication (email, chat, then Skype), and then to conclude offline agreements, and only later online agreements, while agreements continued to be performed mainly in a traditional way. The Internet was seen as a support for the traditional economy and not as a digital economy. Agreements were rarely performed over the Internet and, at first, the process was quite complicated¹² (Barta and Markiewicz, *Handel elektroniczny. Prawne problemy*, 2005).

A significant breakthrough in the development of the digital economy took place in 2007 with appearance of the first iPhone and, most importantly, with a shift in the philosophy of functioning of the Internet, e.g., the appearance of mobile devices and access to the Internet, digitization of assets which used to have a traditional form (music, films, images, photographs, etc. and document digitization), the spread of laptops and notebooks with online access, the first tablets, etc. This significant change resulted from a change in technology and data storage. The shift from open archiving on a computer, through remote access to it, a partial shift to clouds¹³ (Szostek D. r., 2018), (Szostek D. r., 2018) and, finally, a complete shift to storing data in a cloud, data dispersion and, most importantly, removing data from a concrete territory, the ease of transmitting it and then, providing it. Nowadays, you just need online access, e.g., from a mobile device, for cross-border access to all kinds of digital resources or, based on

11 More in: D. Szostek: *Czynność prawna a środki komunikacji elektronicznej*, Kraków 2004, p. 31; A. Wiebie: *die elektronische Willenserklärung*, Tübingen 2002, p. 5 et seq.

12 D. Szostek: *Wykonanie zobowiązania z użyciem środków komunikacji elektronicznej* [in:] *Handel elektroniczny. Problemy prawne*, ed. J. Barta, R. Markiewicz, Kraków 2005, p. 255 et seq.

13 D. Szostek (ed.). *Bezpieczeństwo danych i IT w Kancelarii Prawnej*, Warsaw 2018, p. 290 et seq.

the wording introduced by the EU – digital content, located anywhere in the world. Consumers often lack any knowledge of the location of their data, which is not present, at any given time, in one place, but often in several places, stored in a scattered manner.

Such international technological concerns as Google, Facebook, Amazon and Yahoo or Apple, Microsoft and Samsung, have played a significant role in the creation and development of the digital economy or knowledge-based economy. What is interesting is that many of these entities have been functioning in the market not for a long period of time (e.g., Google since 1998, Facebook since 2004), and their impact on society, e.g., methods of communication, behavior, has been gigantic (e.g., over 2 billion people all over the world use Facebook). It has become extremely easy to perform an agreement online, even from the level of a cell phone or another mobile device. Downloading music or films from the Internet, from any place in the world, has become common. Access to digitized resources of the largest libraries in the world is no longer difficult – you just need to register online – while access to some resources does not even require logging in. This has increased access to knowledge on an unprecedented scale¹⁴. On the Internet, which was initially used mainly for communication and entertainment, there exist the largest bases of knowledge, science and information (with the problem of verifiability) ever created. And the availability and universality of the Internet has caused significant social change, consisting in, among other examples, sharing, using instead of possessing, etc. The so-called generation Y is not as interested in possession or ownership as their predecessors, instead preferring low cost and availability based on new technologies. Their demand is addressed by, among others, streaming applications (access to music instead of owning it), car or bicycle rental companies (instead of buying one), etc., based on technologies and availability (so-called uberisation). The ease of concluding agreements, their cross-border character, or simple payments, significantly contribute not only to the development of services, access to digital content and other digitized resources, but also to cross-border shopping. The issues of applicable law, court jurisdiction and evidence are becoming more and more of a problem. Many people, particularly younger, who use the Internet, do not realize at all the legal acts they perform, not to mention the fact

14 In preparation of this publication, the author also made use of electronic sources, documents and publications, thus allowing it to be written in several locations, away from the home university. Several years ago, it would have taken several times longer to write it than now, mainly due to more difficult access to sources.

that they are performed under the legal regulations of another country. The evidence for performing a legal (conclusion of an agreement) or factual act (its performance, for example, by downloading digital content), is often stored solely in the ICT system of the provider and may be easily deleted or manipulated. For that reason, the ICT projects related to securing evidence, including DLT and blockchains, associated with a new method of recording data, are becoming more and more popular. The issues of providing proper and unchanging, properly secured, evidence is very important in evidentiary proceedings, both civil and administrative. The use of DLT or blockchains provides the opportunity to ensure certainty and an unchanging character of the saved electronic document.

Trends of the digital economy

We are witnessing the development of a new knowledge-based economy, within which industry or production constitute “only” the results. A significant element of that economy is the digital economy fully based on intangible resources and online access. What is interesting is that that economy, unlike industry (based on raw materials and labor) is subject to the principle of growing returns. The principles of the digital economy were described in the so-called “Moore’s law” and “Metcalf’s law”. According to the former (from 1965), computing power (of microprocessors, among others) doubles on average every 18-24 months, which has actually been taking place for over fifty years. Just compare the computing power of a microprocessor of a cell phone and that of the computer that allowed people to land on the Moon. Current phones often have greater computing power than of former “supercomputers”. The latter, i.e., so-called “Metcalf’s law”, states that the usefulness of computer networks is proportional to the square of the number of its connected users. The capacity of two connected computers is much greater than it might seem based on their total computing power. Taking into account both “laws”, the gigantic computing power of contemporary computers and the probability it is going to double over the next two years, and the combination of those computers in networks (which is easily available thanks to current technologies), the fascination of the economy with DLT and blockchains is no surprise.

Before a more detailed discussion of the issues of “blockchains”, we should list the most important trends in the digital economy¹⁵ (Batorski, 2012). One of them is network convergence, i.e., integration of networks that used to be separate. An example is the integration of online services: today we can easily order a product, pay online (using electronic banking networks or the mechanisms of the PSD2 directive), on the basis of an online agreement, etc. Another example is the combination of phone services, online access, digital content, online services, all provided by one entity. The current convergence is associated with the “Internet of Things”, i.e., the integration of “ordinary” items, such as cookers, fridges, coffee makers, into one network with the possibility to control it using one’s cell phone. There are also more serious projects, such as smart gas, electricity or water meters, remote energy networks or the project most important from the point of view of social change and behaviors, developed nowadays: a network of autonomous vehicles. What is very important is that the “Internet of Things” has been applied in recent years in logistics, management of product flow, warehouse inventory and logistics control, including control of vehicles, but also of transported goods. In the “Internet of Things”, information is transferred among “things” automatically and autonomously, without the physical participation of a human being. Blockchain technology is “just” the next stage of the development of convergence.

The other trend is convergence of bits and atoms that introduces the so-called digital industry next to the digital economy. The first stage was integration and transfer of information and documents online, and then of digital content. The current trend indicates more and more frequent use of online production, order customization, etc. An example is the production of goods using a 3D printer, where product content is sent online (such printers are used for, among other purposes, manufacturing elements of airplanes, cars, etc.). What is also noticeable is the tendency to customize the product, but also to eliminate people (labor) from the process of production.

Another trend that is already present in the modern economy is data processing and storage in clouds, both for business and private purposes. It is associated with people’s growing mobility. Computers, laptops, tablets

15 See also the report “Digital Economy. Key trends of the digital revolution”, ed. D. Batorski, http://www.euroreg.uw.edu.pl/dane/web_euroreg_publications_files/1335/cyfrowa_gospodarka_kluczowe_trendy_rewolucji_cyfrowej.pdf of 15 June 2018.

and phones are becoming terminal devices, while content is more and more often stored away from those devices. On the one hand, we are becoming dependent on the provider of cloud-computing services, while on the other, data security increases. Loss or failure of a device does not cause irrecoverable loss of data or access thereto. There is also visible the tendency for dispersing data in the network, out of touch with the physical territory of (the country) processing the data. An example might be the Microsoft Office 365 software which is cloud-based, where access to documents takes place from any device with the installed access application, as long as it is connected to the Internet. The first stage was transferring data from computer disks to the servers of professional server rooms, often for backup purposes. Then, the main resources were transferred to external servers, data was transferred to foreign servers and, finally, data was transferred to ICT systems in the form of distributed data recorded on multiple servers in many places in the world, not in contact with any physical territory, which is becoming more and more similar to the so-called autonomic cyberspace. A serious problem is dependence on one provider. The blockchain is another stage associated with transferring to clouds and limiting the monopoly of the provider.

The sharing and service-based economies are other important elements of the digital economy. The trend of the need of availability replacing the need of ownership is becoming more and more visible, in particular among young and very young people. Applications and new technologies allow the use of things but, most importantly, provide full access to them in a manner similar to ownership. Such an approach is related to transferring goods to clouds, but also to the habits associated with joint participation in global ICT systems. The generations raised and strongly functioning in the traditional economy are characterized by a prominent need for ownership, both of things and “ownership” of digital content. The result is purchasing CDs, downloading music files to one’s own devices, installing software on devices, having one’s own cars, bicycles, etc. Sharing consists of full access without “appropriating” or full authority over things or digital content. Instead of purchasing a CD with music or a film or downloading data to one’s own device, there is full online availability, for example by streaming. Instead of purchasing a book (in paper or digital form), there is subscription and online access to books. Instead of one’s own bicycle, we can rent one and share it with others when we don’t need it, which is no longer surprising for anyone. Just like sharing a car (e.g., renting a vehicle with payment by the minute), we can share an apartment – home swap-

ping is provided by a number of websites, such as Intervac or HomeExchange2.

Another stage is autonomous vehicles which, most probably, will not be owned by a single person. They will be available in the time similar to “driving a traditional car out of your garage”. That trend is an obvious combination of: data convergence, the Internet of Things, digitization and development of the digital economy, transferring data to clouds and network convergence. The ownership-based model of the economy is transforming into a model based on services and availability. The SaaS Software is a Service model instead of a single purchase, a service payable periodically, based on demand. And, again, the blockchain seems to be “just” another, but more and more essential, element related to the trend of sharing.

The decreasing significance of intermediaries and activity platformation are the next strong trends of the digital economy. The development of eCommerce has been primarily based on that trend. Resigning from, or minimizing the use of, intermediaries is the basic objective of business-process optimization. That process is progressing fast. Instead of distribution, with a producer, importer, domestic distributor, wholesaler, regional seller and end seller, that process is shortened to producer, domestic distributor and seller or even producer – seller, producer – end user. The latter trend is particularly visible in the field of digital content (e.g., you can purchase a Windows software license directly on the Microsoft website), where intermediaries are practically eliminated. The manner of distribution is also changing, new channels are developing, and so are new services, e.g., short-term apartment rental. Where it is impossible to eliminate intermediaries, they are significantly changing into fully computerized entities, online platforms that allow someone to perform an activity in real time. Examples include Amazon, eBay, Booking.com, or the Polish website Allegro which allows a customer to conclude a cross-border agreement, pay, and also to verify the purchased product or service. What also plays a role is the guarantee and complaint procedures provided by these platforms. Tokenization, and thus blockchain technology, result from that trend. Cryptocurrencies were developed and introduced under the slogan of eliminating intermediaries. It is not completely true because, in practice, previous intermediaries were replaced by new ones, such as cryptocurrency exchanges, miners collecting fees for providing computing power, etc. Platformation or convergence have changed the principles of competition, introducing global competition in place of local competition. Online availability of digital content, as well as ease of buying and delivering traditional goods, even from the other side of the world, and also the popularity of the Eng-

lish language, standardization of processes, services and products, result in a situation in which entrepreneurs act, more and more often, on a global, and not a local, scale. Examples include App Store, Amazon, Alibaba and Booking.

Other visible trends include crowdsourcing, or allowing consumers to make decisions, and prosumerization, i.e., entrusting consumers to perform more and more tasks, so that they provide the services or develop content themselves. DLT and blockchain technologies are mainly based on these two trends.

Another visible change in the modern economy is automation and replacing the work of people with the work of machines, computers, robots and artificial intelligence. It is a direct result of the industrial revolution of the previous century which replaced first the work of animals, and then of people, through the application of machinery. Digital economy automation not only eliminates physical labor, but typically also intellectual work and a number of services. It is particularly visible in the fields of banking and finance where, in combination with crowdsourcing and prosumerization, it has significantly impacted employment. Artificial intelligence and big data have seriously affected analytics and projection and have also impacted and developed convergent projects which would have been considered science-fiction just several years ago (e.g., developing a network of autonomous vehicles). That tendency significantly affects the development of so-called technological unemployment which we are going to have to face in the foreseeable future¹⁶.

Taking the above into consideration, the tendencies of recent years associated with the creation of cryptocurrencies away from the banking system, tokenization of multiple activities, including obtaining investment funds through ICO¹⁷, are no surprise. Traditional issues of securities are being replaced with virtual (digital) issues, in a way bypassing domestic regulations¹⁸. It is a consequence of all the other tendencies and, in a way, immortalizes them, but in the eyes of employees it seems surprising and requires serious analyses of the law, of social behaviors, new legal and financial instruments, as well as assessment of their impact on legal regulations.

16 Prepared based on the report “Digital Economy. Key trends of the digital revolution”, ed. D. Batorski, http://www.euroreg.uw.edu.pl/dane/web_euroreg_publications_files/1335/cyfrowa_gospodarka_kluczowe_trendy_rewolucji_cyfrowej.pdf of 15 March 2018.

17 ICO (Initial Coin Offering) – contemporary crowdfunding that consists of collecting capital via start-ups, using cryptocurrencies or tokens. See also below.

18 See also below.

DLT and blockchains as a catalyst for lex electronica?

Technology, particularly its convergence in the digital economy, the cross-border character of concluded agreements, the lack of physical borders for online activity and state-of-the-art technological novelties, such as tokens and so-called tokenization of actions, ICO, smart contracts (self-implementing), cryptocurrencies, including Bitcoin, DLT and blockchains, big data and IoT, are just some of the tools that may replace or have already replaced the law in many statements (mainly by economists and IT specialists). The latest technological tools have certainly changed human behavior and the manner of concluding and performing agreements, have introduced new tools unknown before (such as tokens) which, however, is a modern substitute for previous legal instruments (to be elaborated on below). The question appears of whether they will actually revolutionize the previous legal principles, will affect them, will allow the development of the concepts related to a separate legal system, the so-called *lex electronica* or cyberspace, or whether they will become just a modern instrument, a tool that just modernizes the principles of the law we have known so far. The appearance of the Internet several years ago also gave rise to predictions of revolution in the law, while in fact previous rules have worked perfectly with new technologies which, however, have changed the previous interpretation of laws, caused a number of legal issues and doctrinal disputes, also leading to significant evolution of legal views and regulations and to completely new legal concepts and legislation. However, they did not replace previous achievements, supplementing and slightly modifying them instead. New technologies have also required new legal solutions, mainly associated with the online environment, at first on a local (domestic) scale, and then, at a community scale¹⁹. Will DLT and blockchains cause legal changes on a global scale considering they are applied on a global scale, or will they change little?

The concept of autonomous law in cyberspace is much older than the technical solutions allowing its implementation, and dates back to the early days of Internet development on a global scale. It is supported by, among others, D.R. Johnson and D.G. Post²⁰, who stated:

19 An example is personal data protection which was first regulated locally, while now it is regulated in the EU with a regulation directly applicable to all the EU legal systems.

20 D.R. Johnson, D.G. Post *Law And Borders – the Rise of Law in Cyberspace*, *Stanford Law Review* 1996, No. 48 p. 63 (Johnson i Post, 1996 nr. 48); D.R. Johnson,

“Regardless of the doctrine attached to territorial jurisdictions, there will appear new principles applicable to a number of electronic activities, managing the whole spectrum of new phenomena, without direct equivalents in the real world. The new principles will perform the role of laws, by defining legal personality and ownership rights, used for solving disputes and contributing to development of positions regarding the fundamental, common values” (Johnson and Post, 1996).

The concept of separate cyberspace law refers mainly to eliminating the doubts regarding jurisdiction and applicable law, as well as the distribution and flow of goods in the digital world²¹. A similar view is presented by promoters of DLT and blockchain technologies in the scope of, for example, distribution of digital content and so-called virtual property. D.C. Menthe²² (Menche, 1998) suggests cyberspace should be considered international space. He believes that the previous principles of jurisdiction and applicable law are not sufficient for the Internet and that it is necessary to create a new, separate, legal area. In his opinion, jurisdiction should be solely based on a personal criterion²³, cyberspace as an ex-territorial area, commonly owned by all countries. The concept of Lex electronica was presented by Pierre Trudel²⁴ (Trudel, 2001) who suggested not only the development of cyberspace but also the functioning in it of a lex electronica, or electronic law, separate from domestic law, and applicable mainly to virtual goods. That concept mainly refers to law of the contracts concluded online. A similar concept, but in the scope of copyrights, was presented by Vincent Gautrais²⁵ (Gautrais, 2016). (Railas, 2004). The attractiveness of these concepts mainly consists of eliminating doubts regarding jurisdiction or choice of applicable law for the contracts concluded or performed online, but also in providing the opportunity to develop new legal structures

D.G. Post The New “Civic Virtue” of the Internet, the Emerging Internet – 1998 Annual Review of the Institute for Information Studies, 1998.

21 Kulesza, J. (2010). *Międzynarodowe Prawo Internetu*. Poznań, p. 291.

22 D.C. Menche, Jurisdiction in Cyberspace: a Theory of International Spaces, \$ Michigan Telecommunications and Technology Law Review 1998, No. 69 pp. 69-103.

23 Kulesza, J. (2010). *Międzynarodowe Prawo Internetu*. Poznań, p. 299.

24 P. Trudel: La lex electronica w: Le droit saisi par la mondialisation, ed. Ch. A. Morand Bruksela 2001, p. 221.

25 V. Gautrais: Lex Electronica: d’aujourd’hui a demain 2016. <http://www.lex-electronica.org/articles/volume-21/lex-electronica-daujournhui-a-demain/>. The issue of lex electronica is also indicated by L. Railas: The Rise of Lex Electronica and the International Sale of Goods, p. 500 et seq.

only for the Internet or, more broadly, for the digital economy. There also appear more utopian concepts indicating that the Internet is a space of complete freedom, where the main principles include open source and everyone's right to all the content published online (in practice, the elimination of copyrights as we know them). Publishing something online would be tantamount to allowing all Internet users to use it. These concepts are significantly inconsistent with the principles and trends of the digital economy which, in fact, is based on the exchange of goods (payment and the right to use personal or other data).

At the level of the European community, there has appeared the concept of a separate legal regime for contracts concluded online. It was to be a legal regime separate from the domestic system, both available for the consumer to choose from. The choice was not to constitute choice of applicable law, but rather as choice of domestic law, e.g., the Polish Civil Code or an EU regulation. That concept was transformed into the real-life draft regulation of the European Parliament and Council regarding European sales provisions which, in practice, contained uniform provisions of the general part of civil law and of the general part of liabilities, as well as the issues regarding sales agreements (including for sale of digital content) and liability for defects. The regulation was limited to sales agreements, agreements connected with digital content and services related to it, and was only to apply to online contracts concluded on a cross-border basis. In the end, despite its complementary character, the draft was not adopted.

The concepts based on DLT and the blockchain as the tools allowing the development of a new order in cyberspace, without the participation of previous institutions or authorities, based on completely autonomous and democratic activities, with the Internet-user community responsible for supervision (the concept on which Bitcoin is based) instead of the institutions applying domestic law, are nothing new. They should rather be considered a reflection of previously developed concepts or of the whole philosophies of the new order based on a cybernetic society. People are often incorrectly think that performance of an act online, e.g., tokenization of an action or smart contracts of ISO replace, as factual activities, legal regulations, or that legal regulations do not apply to them. – cyberspace based on DLT or blockchains, deprived of legal regulations, based on technological factual acts as the space of functioning of the digital economy. Such an approach seems highly revolutionary or even, despite its superficial attractiveness (as fulfilment of the idea of democratization of society and of the activities undertaken by it), dangerous for people using new technologies and functioning in the digital economy.

We should start from the concepts of agreements that justify their binding character. A deeper analysis indicates many consistencies of those with the contemporary ideas based on technological tools.

Contract as a social phenomenon was developed independently of the law, in the societies that did not know the notions of state or law. From a historical point of view, it applies both to indigenous people and, in our times, to newly discovered (although less and less often) tribal groups. Originally, contracts were associated with various forms of adoption, issues of purchasing wives and including them in tribes, but also with the compensation system that replaced blood feuds. It was only in time that the importance of contracts shifted towards trading in goods (barter), then trading in goods in exchange for money and, later on, contracts became regulated in accordance with common law, and later with codified law²⁶ (Weber, 1960) (Radwański, 1977). It seems that cyberspace is taking a similar route nowadays, where a number of contracts, as well as behaviors, are generated as customs on account of lack of regulations in the form of codified law. These customs more and more often transform into the so-called soft law as well as into standards (often technological ones) such as, for example, the standards determined in the ISO system which are first voluntarily accepted as support or guidelines for conduct, and finally they are included in a legal framework (at the local or supralocal level or as so-called guidelines). In cyberspace, customs are very important elements affecting the contracts concluded in the electronic environment or associated with the electronic environment. An example indicating the pattern of creation of the law associated with digital economy is the development of a contract for storing data in a cloud. At first, the contracts were based on the principle of freedom of contracts and often, depending on the parties, there were significant differences among the contracts. Gigantic legal doubts and problems related to cloud storage led to the development of opinion 5/2012 of the Article 29 Working Group of 1 July 2012 on cloud computing, then the Sopot Memorandum of the International Working Group on Data Protection in Telecommunications (the so-called Berlin Group), the consequence of which was the “cloud contract” EU strategy²⁷. In response

26 M. Weber, *Rechtssoziologie*, Neuwied 1960 p. 110 et seq. Z. Radwański: *Teoria umów*, Warsaw 1977, p. 7 et seq.

27 Communication of the Commission to the European Parliament, European Council, Economic and Social Committee and Committee of the Regions “Unleashing the potential of cloud computing in Europe” of 27 September 2012. KOM (2012) 529.

to the above-mentioned soft law, the standard ISO 27018 was prepared regarding data security in the cloud, indicated as a necessary tool in connection with, among others, the execution of the GDPR.

It seems that not only the development of customs, but also other elements developed within the law-of-nature concept²⁸ (Jorgensen, 1968), may be found in the contemporary theories regarding new technologies and cyberspace, although the law-of-nature concept developed mainly on the basis of Roman consensual contracts, as well as knowledge of the freedom of people.

”It was based on the assumption that the act of will of its participants constitutes not only the necessary, but also sufficient, element of every agreement. The liberal trend of law of nature then developed the theory of primal and inalienable freedoms of people. Under that theory, only the entity itself could, through its own will, impose on itself any restrictions, while the agreement had the basic function of social integration and coordination of human activity ... It is because only an agreement can make people cooperate without violating their freedom. Although an agreement is to bind its participants, that effect results from their free decisions that guarantee its moral acceptance”²⁹.

That concept developed into a civilist theory of autonomy of will³⁰ (Kant, 1971). It stated that the very individual will plays a shaping role in the scope of legal relations, because it is characterized by the proper creative force. That was to constitute the autonomic character of individual will. As a result, that theory assigned a secondary role to positive laws. Their function was to consist not only of protecting the laws developed through the autonomous will of people, but of not requiring any concession or acknowledgment by the effective legal system. Provisions of the law express the tacit consent of the parties. The theory of autonomy of will proposed the principle of freedom of contract and led to a number of theses: People have full freedom in whether to conclude a contract or not. They may freely develop the contents of a contract and, in particular, do not have to follow the nominate contracts regulated in statutory law. The legal relationship resulting from the contract may be later changed by the parties.

28 On the law of nature: S. Jorgensen, *Vertrag und Recht*, Copenhagen 1968, p. 61 et seq.

29 Radwański, Z. (1977). *Teoria umów*. Warszawa, p. 9.

30 Term coined by E. Kant: *Uzasadnienie metafizyki moralności*, Warsaw 1971, p. 78.

What is decisive for determining the legal consequences of the contract is the actual will of the parties, even if it is not consistent with their declarations of intent. The contractor that has not received the consideration due from the other party may request protection from public authorities as if performing a contract. In the case of a conflict of laws, the parties may choose the act to be applied to the resolution of the case associated with the legal relationship developed by the contract. Informal agreements evoke full legal consequences³¹.

The enthusiasts of the theory of autonomy of will indicated that using one's freedom may not result in its self-destruction. The autonomy of one person may not violate the freedoms of another person without the consent thereof. It would violate the principle of equality which, in the doctrine, is connected to the requirement of protection of freedom.

Other theories justifying the will of a person as the foundation of a contract include: the sociological (functional) theory, psychological theory, theory of reborn laws of nature and phenomenological theory. The sociological theory includes an interesting concept of a "living law" by E. Ehrlich³² (Ehrlich, 1918) in which the laws comprise a certain order developing in various social groups (such as Internet users) regardless of the standards established by the state. Legal order is determined through various legal facts, including, among others, contracts. These facts are taken into account by courts taking into account interests *in concreto* and constitute, by themselves, sources of legal obligations. These are the foundations of the binding force of contracts, and the consequences are described by the abstract and general legal norms established by the state only apparently. It is worth quoting another promoter of that theory, H. Isay³³ (Isay, 1929) who stated that the connection between the factual condition (including the agreement) and legal effects results not so much from a positivist standard, but rather that there appears a sort of legal feeling, i.e., experience of social character. The phenomenological theory of laws by A. Reinach (Reinach, 1913) is similar to the theory of "reborn laws of nature".

"The author was seeing the foundations of the legally binding character of contracts in the a priori categories, existing away from space or time, which are impossible to explain anymore. However, we may, and should, describe more closely the act of "promising" which, by itself,

31 Radwański, Teoria umów, p. 20.

32 E. Ehrlich; Die juristische Logik, Tübingen 1918, p. 280.

33 H. Isay: Recht und Entscheidung, Berlin 1929, p. 5.

results in the obligation of the promisor and in a claim, correlatively connected to it, on the part of the addressee of the expectation.”³⁴

The above-mentioned, briefly presented, theories, stand in strong opposition to positivist theories, including the historical school of F. Savigny or normativism, based on legalism and legal norm as foundations of contracts.

This brief review of the concept related to “sources of binding force of contracts” indicates that the contemporary concepts, based to a high degree on technology, or rather on fascination with its possibilities, related to cyberspace, e.g., *lex electronica* or the concept of automation of cyberspace law, are not far away from the theory of the source of the binding force of contracts from over one hundred years ago, and many discussed issues regarding the binding force of those contracts may be explained, with ease, using the already existing and comprehensively discussed theories. It even seems that, nowadays, the developing global society, functioning both in the space of the respective states (physical functioning) and globally in cyberspace in a way out of touch with physical territory, while performing a number of legal acts, including by concluding a number of contracts, is becoming a practical “entity” that makes it possible to “test” the above-mentioned concepts and theories in practice. It is necessary to highlight the fact that, depending on context, the “global society”, as well as the so-called digital economy, are at different stages of development.

As regards the DTP and blockchain technologies, we are currently at the stage of development and significant standardization of customs (as indicated by the initiatives related to blockchains) which will probably and quickly develop into ISO norms that are going to constitute the standards for technology as well as for the contracts associated with them. Standardization, particularly in technical terms (but not only), in the environment not regulated online, as well as soft law, are becoming permanent elements of norms, including legal ones (regardless of the source of their effectiveness), despite the lack of a uniform lawmaker or regulator. The difference associated with the procedure of development of common law (in the societies deprived of laws ages ago and the contemporary society of Internet users), and then its sanctioning, is the space (cyberspace), in which cus-

34 Z. Radwański: *Teoria umów*, p. 26.

toms are developed and sanctioned with unprecedented speed³⁵. The states or supranational institutions which developed, within the positivist approach to sources of contracts, the legal norms and social behaviors, in the global economy are replaced by global concerns that develop ICT systems but also legal principles (among other regulations) imposing principles of conduct on vast numbers of people (millions or even billions). Examples include FB or LinkedIn. Paradoxically, they limit the will of the individuals using those systems to the behaviors predefined in the software (ensuring, using technological means, that the acts not allowed in the system may not be performed). A simple example is the inability to publish content in a portal in a format other than that allowed by the system, and also the manner of functioning of “smart contracts”.

The issue of institutional control and performance of online contracts, as well as pursuing claims related to them, is resembling, more and more, arbitration, including online, fully electronic, arbitration (so-called Online Dispute Resolution (ODR))³⁶ (Szostek and Świerczyński, *Arbitraż elektroniczny*, 2007). ODR is a modern version of ADR (Alternative Dispute Resolution which has been used for decades, in particular in international trading). ODR is characterized by low costs, ease of submitting complaints as well as of filing documents, speed, delocalization and the elimination of the limits of space or time. Practically speaking, all you need to conduct the whole proceedings is online access³⁷ (Schultz, 2006) (Kaufmann-Kohler and Schultz, 2004). The EU regulated the functioning of ODR in regulation No. 524/2013/EU and directive 2012/11/EU. It works on the basis of

35 The global character of cyberspace is not uniform. There are several zones – different in terms of the technologies applied, territorial scope and also scope of control, and thus freedom and access to the Internet. Western societies (one of the zones) are used to freedom in using the network. The freedom is quite different in Russia and in the countries dependent on Russia, while China, with hundreds of millions of Internet users, exercises full control and significant restrictions. What is interesting from the point of view of history is that the cyberspace zones overlap, to a large degree, the spheres of influence of Western countries, Russia and China. This issue significantly exceeds the framework of this study, so it was only briefly indicated, while the term “global character” will be used hereinafter, despite being aware of a lack of a uniform character of cyberspace.

36 More on development of ODR in. D. Szostek, M. Świerczyński: *Arbitraż Elektroniczny*, KPP 2/2007, p. 471 et seq.

37 T. Schultz *Information technology and arbitration. A practitioner’s guide*, Wolters Kluwer International 2006. p. 5 et seq.; Gabrielle Kaufmann-Kohler, Thomas Schultz: *Online Dispute Resolution: Challenges for Contemporary Justice*, Wolters Kluwer International 2004, p. 11 et seq.

proper contractual provisions outside of the EU, including in B2B transactions. What is important is procedure simplification and speed of conduct, which encourages more and more parties to choose that form of dispute resolution over traditional courts. As regards disputes related to cryptocurrencies or tokenization – ODR is about to become the standard for their resolution. One of the advantages of DLT and blockchain technologies is the non-repudiation, permanence and guarantee of authenticity of the contractual provisions made using them which, to a high degree, translates into a guarantee of evidence in case of a dispute. Certainty of the fact secured in the discussed technology will contribute even more to the development of ODR, in particular for international disputes.

Therefore, social behaviors in cyberspace, tokenization of contracts, their new types, establishment of cryptocurrencies and social (democratic) control of the data recorded using blockchain technology are nothing new in terms of the theory of the source of contracts. The scope (billions of people), space (no physical territory) and speed of change are different, as are the development of principles by global concerns, process technologization and the manner of solving disputes. Courts are being replaced with the ODR procedure, including online mediation or arbitration. It is becoming common practice to submit disputes related to cryptocurrencies to ODR, in particular due to the problems of jurisdiction and applicable law. There are a lot of arguments proving that also other activities based on DLT and blockchains, in particular the services developed by global concerns and international initiatives, are going to be subject to online arbitration in case of disputes, instead of decisions made by traditional courts.

Taking the above into consideration, we might venture to say that, next to the traditional attitude to agreements, roles of states and courts, there is appearing a new area that is not going to eliminate the previous method of functioning based on codified law and common courts, but is rather going to function simultaneously, by means of cyberspace and electronic communication.

Chapter II. Blockchains, DLT – basic terms.

It would be impossible to attempt to discuss the legal issues of using DLT and blockchains without first defining a number of technological terms used in this study, as well as in the publications, discussions and reports connected with the digital economy. The difficulty is connected to the technical character of these terms and to a lack of uniform legal definitions due to their innovative character. Many remarks regarding DLT or blockchains result from a wrong understanding of those terms or from different points of view, depending on the profession of the speaker. The purpose of the following proposed definitions is to present the issues to lawyers and to present the conceptual framework used in this monograph, as well as to indicate how that issue was solved in the statutory laws of certain states³⁸.

DLT – distributed ledgers

Definition

Development of informatization may be divided into several stages. At the beginning (when computers were gigantic, but with very poor computing power in comparison to contemporary mobile devices), calculations and other data were stored locally, on one computer³⁹. Additionally, at that time it was impossible to transfer data (apart from physical transfers of the punched tapes used for programming the first computers). Development of information technology was dependent on the development of commu-

38 This study is not of a legal comparative character and for that reason only solutions from some of the states are presented.

39 The ENIAC (Electronic Numerical Integrator and Computer) was considered, for a long time, to be the first computer in the world (it is no longer so obvious after declassification of British documents – there is the issue of precedence of such machines as Colossus or ABC), was 12 meters by 6 (in the shape of the letter U), of a height of 3 m and a width of 0.6 m. It contained 18,000 electron tubes, 6000 commutators and 50,000 resistors. It weighed 327 tons and had no operating memory. It was only the 1947 invention of the transistor that allowed the size of computers to be reduced and an increase in their computing power.

nication⁴⁰. The possibility to connect two and more computers allowed a significant improvement of their computing power. The so-called “Metcalfe’s law” states that the usefulness of computer networks is proportional to the square of the number of its connected nodes. In turn, a *computer network node* (a so-called *node* – a term significant for blockchains) is an active electronic device connected to the network which allows the sending, receiving and transfer of information through a channel of communication⁴¹. In 1964 Paul Baran, in his memorandum⁴² RM-3420-PR “On distributed communications: I. Introduction to distributed communications networks” (Baran, 1964) published the breakthrough concept (in just 37 pages) of information distribution.⁴³

He indicated and proposed (by presenting suitable calculations) a decentralized and distributed method of connecting nodes (devices) and sending data (the blockchain was developed much later, on the basis of that concept). He classified (data-distribution) networks into three types: centralized, distributed and, within that category, decentralized networks.

A *decentralized network* (most commonly used by regular users at home or by employees in small offices) is a network, in which all the nodes (i.e., devices) communicate (send) data to the central node (server), from which it is sent to other nodes (devices).

A *distributed network* does not have a central server, and transfers data using the shortest route possible⁴⁴.

Within a distribution network, P. Baran suggested a *decentralized network* (being a type of distributed network) with multiple nodes, of which some are supernodes, but not servers.

40 About a dozen years ago, it was difficult to send larger data packages between regular computers. Today, online access to data, of significant size, is easy and cheap thanks to the development of communications, optical fibers and mobile communication.

41 A combination of computer, phone and tablet – in total three (or four, if you add home server) nodes of a computer network. A server is a node connected to a large number of other nodes.

42 P. Baran: On distributed communications: I. Introduction to distributed communications networks, Santa Monica 1964, pp. 1-37.

43 Source P. Baran: On distributed communications: I. Introduction to distributed communications networks, p. 2.

44 See P. Baran: On distributed communications, pp. 8-9.

The term “DLT” (distributed ledger technology), was introduced in “A report by the UK Government Chief Scientific Adviser” in 2015⁴⁵ (publication in January 2016).

According to its authors: “Distributed ledgers are a type of database that is spread across multiple sites, countries or institutions, and is typically public. Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when the participants reach a quorum. A distributed ledger requires greater trust in the validators or operators of the ledger”⁴⁶.

In DLT, we can develop the so-called *shared* ledgers (a term coined by Richard Brown)⁴⁷, or bases (data or applications) shared by certain entities or by a consortium (they may also be commonly available). In shared ledgers, layers of authorizations are developed for different users.

Legal definition

Two years after the term DLT was coined, it was assigned a legal definition.

One of the territories that introduced the definition of distributed ledgers is Gibraltar which, in its Financial Services Regulations 2017 of 12 September 2017 (it took effect on 1 January 2018),⁴⁸ defined it in the following way (point 2 of the Regulation):⁴⁹

45 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf access from 12 November 2018.

46 In a centralized system, there is one entity that makes decisions on the entry, who needs to be trusted. An example of a system of acceptance by users may be a logistics system, e.g., a producer, supplier or several suppliers, intermediary, end recipient, etc. Delivery of a product includes the respective stages, e.g., the product is collected by the intermediary that sends information, within DLT, to all the participants (producer, supplier or suppliers, end recipient) who verify the given item and the information on it (e.g., where it was sent, whether the item is consistent with the information provided, etc.) and if the information fits the processes that were to be performed on the given item (in the real world, we verify whether the documents are correct) then the given processes are accepted and approved. Everything takes place instantaneously (practically at the same time) and automatically, through devices connected via nodes.

47 See A report by the UK Government Chief Scientific Adviser.

48 Gibraltar Gazette, No 4401. [http://www.gfsc.gi/uploads/DLT%20regulations%20121017%20\(2\).pdf](http://www.gfsc.gi/uploads/DLT%20regulations%20121017%20(2).pdf) of 23 June 2018.

49 <http://gibraltarlaws.gov.gi/articles/2017s204.pdf> of 24 June 2018.

“distributed ledger technology” or “DLT” means a database system in which – a) information is recorded and consensually shared and synchronized across a network of multiple nodes; and b) all copies of the database are regarded as equally authentic.

In July 2018 (5th July), the Maltese lawmakers adopted a set of acts regarding blockchains. In the Malta Digital Innovation Authority Act C901⁵⁰, it defined “DLT”, “distributed ledger technology”, in the following manner: “‘decentralised ledger technology’ means a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes, or any variations thereof, as further described in the First Schedule of the Innovative Technology Arrangements and Services Act, 2018, and the term “node” means a device and data point on a computer network”; under which software and architectures which are used in designing and delivering DLT which ordinarily, but not necessarily: a) uses a distributed, decentralized, shared replicated and ledger, b) may be public or private or hybrids thereof; c) is permissioned or permissionless or hybrids thereof; d) is immutable; e) is protected with cryptography; and f) is auditable.

DLT and documents

The DLT (distributed ledger) technology is closely connected to the latest concepts of understanding the term “document”, under which authorized information is more important than the formal document containing it, so-called “access to information in place of document⁵¹” (Szostek D., *Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej*, 2012). The essence of a document may be seen in the recording of information in a relatively permanent manner, so that it is possible to disclose it, reproduce it, copy it or transfer it to another medium in an unchanged condition. In the doctrine, but also in the judicature, there are listed several basic elements of a document: 1. medium 2. information 3. recorded so as to allow someone

50 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=1> of 11 November 2018.

51 See D. Szostek *Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej*, Warsaw 2012, p. 26 et seq.

to get to know its content⁵². For hundreds of years, documents were recorded in a tangible form (clay tablets, parchment, paper, etc.), with a kind of physical unity of the (tangible) medium and the information recorded thereon. Digitization, and the resulting paperless format, is consistently leading to a change in one of the elements of a document, i.e., its medium⁵³. It is worth noting that since 1 July 2016, under art. 3 point 35 of the eIDAS regulation, applicable directly to all the legal orders of the EU countries, an electronic document is any content stored in electronic form, in particular a text or a sound, video or audiovisual recording. The term ‘medium’ is neutral and not necessarily connected to its traditional, physical meaning, which is visible in the recent evolution of that term⁵⁴, including recording in clouds, or in a distributed manner.

In the first stage of digitization and digitalization of documents, traditional (paper) documents became accompanied by electronic documents, saved in one file, depending on the need, legal requirements, but also the applied method of protection (of their authenticity and integrity), the type of applied IT tools, e.g., as a pdf or signed using PKI (public key infrastructure), including using secure electronic signatures and, since 2016, qualified electronic signatures. Such a document was often printed and sent to the addressee in a traditional way. In the next stage, the electronic document started being sent using electronic means, usually emails, and the response was sent to the sender in the same way (or using traditional mail). Such a model may be compared with a centralized network, where information is sent out and in to the same point. However, each participant has a different set of documents (depending on what documents it receives and sends and to whom).

The next stage, associated with the growing speed and size of the data possible to send was (or even, in the less developed digital economies, including Poland, is) transfers of documents to clouds – the next stage of development of the digital economy. At first, transferring to clouds was, or is, connected with creating backup copies while leaving the primary document on its own data carriers. Successively, however, the main resources were, or are, also transferred to clouds, with the terminal device (computer,

52 D. Szostek: [in:] *Informatyzacja postępowania cywilnego. Komentarz*. Warsaw 2016, p. 69 et seq.

53 See also D. Szostek: *Informatyzacja postępowania cywilnego. Komentarz*. Warsaw 2016, p. 74; D. Szostek, *Nowe ujęcie dokumentu*, 2012, p. 52 et seq.

54 See also the chapter of this study *Blockchains and durable media*.

phone, tablet, etc.) as the access device that does not store data or documents⁵⁵. That system continues to be a centralized one.

In time, there appeared the concept of sharing documents and of interactivity which resulted from, among others, a different approach to documents and to the manner in which they are stored, i.e., not as a complete thing but as data that may be accessed using the proper software⁵⁶.

In DLT, it is not so much documents (as whole files) that are sent, but rather the respective pieces of information (data) is recorded simultaneously (in real time) in all the nodes (devices) participating in the information exchange. Therefore, everyone has exactly the same data in real time, in the scope in which they have access to it.

Information verification takes place automatically through IT systems based on cryptography and data-transfer protection⁵⁷. That information is approved after verification by the persons (or nodes – devices) authorized to it, e.g., the node of the given state, local authority, etc. It is possible (although impractical) to introduce the mechanism of acceptance by specific natural persons.

In practice, that process is similar to the process of making entries in a ledger which has been known for decades. In the latter process, using a document specified by legal provisions, drawn up by the authorized person (e.g., a public notary drawing up a notarial deed (in DLT – an authorized node)), other persons after verification of that document (e.g., judges in a court (node authorized to verify)), they enter (accept) the data, for example, in a land and mortgage register or another ledger, from which other entities (e.g., the authorized nodes) may collect it (but not accept it). In the case of DLT, everything takes place in real time, usually automatically, and the data is not entered in one ledger, but in many, depending on the level of authority. Everything is secured cryptographically. Also verification, control and acceptance are cryptography-based.

DLT allows the recording of information in ICT systems in a fast, effective and secure manner (cryptography in place of traditional documents).

The advantage of such data sharing and of assigning authorizations is also emphasized in the English report entitled “Distributed Ledger Tech-

55 This is supported by a number of arguments, such as security, etc. However, there are also many opposing arguments. That issue, however, exceeds the scope of this publication.

56 D. Szostek, *Informatyzacja postępowania cywilnego. Komentarz*. Warsaw 2016, p. 77.

57 See also the technical aspects in the point devoted to the definition of a blockchain.

nology: beyond block chain. A report by the UK Government Chief Scientific Adviser? Distributed ledger technology uses keys and signatures for control purposes and to assign authorizations to specific entities within the shared ledger. These keys may be assigned to specific functions on certain conditions only. For example, a regulatory authority may have the key that allows observance of all the transactions of an institution, but only if the key, held by the court, provides it with such authorization. (...) Records are added using a unique cryptographic signature which confirms that the authorized user added a suitable record in accordance with certain regulations”⁵⁸.

Blockchains

Definition

The term 'blockchain', earlier 'block chain', is already 10 years old. It was first used by a group of IT specialists/enthusiasts but, with the growing popularity of Bitcoin and other cryptocurrencies, has become successively more and more commonly used, becoming one of the most popular terms used in 2018. The concept of the origin of blockchain technology dates back to 2008 and to the publication of a white paper on cryptography by the person or persons operating under the nickname Satoshi Nakamoto⁵⁹ (Satoshi, 2018) (Ducas and Wilner, The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada, 2017). The document proposed the introduction of an electronic version of money, allowing direct peer-to-peer (P2P) payments so as to eliminate participation in the payment system of central authorities and intermediaries. That technology was to (and currently is) based on blockchain technology. However, the very concept of using cryptography dates back practically to the beginning of computerization. In turn, the idea for a cryptographically secured chain of transaction blocks was described by Stuart

58 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf of 12 November 2018.

59 Satoshi Nakamoto: “Bitcoin: A Peer-toPeer Electronic Cash System” 2008r. <https://bitcoin.org/bitcoin.pdf> of 9 November 2018.; E. Ducas, A. Wilner: The security on financial implications of blockchain technologies: Regulating emerging technologies in Canada, International Journal, No. 72/2017, p. 544 (cited as: “E. Ducas, A. Wilner, 2017”).

Haber and W. Scott Stornett in 1991⁶⁰ (Haber and Stornett, 1991) and developed by R. Anderson⁶¹ (Anderson, *Security Engineering: A guide to Building Dependable Distributed Systems*, 2008) (Anderson, on: *Security Engineering: A guide to Building Dependable Distributed Systems*, 2001).

A report for the British government⁶² (Walport Mark (przedmowa), 2015) indicated that a blockchain is a type of database that takes a number of records and puts them in a block (rather like collating them on to a single sheet of paper). Each block is then ‘chained’ to the next block, using a cryptographic signature. This allows blockchains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions.

There are many ways to corroborate the accuracy of a ledger, but they are broadly known as consensus.

In another report, Deloitte Australia⁶³ indicates that a blockchain is to be understood as a distributed book used for recording and sharing information in peer-to-peer networks. Identical copies of a ledger are maintained and jointly verified by network members, and the accepted information is aggregated in “blocks” that are added in a chronological “chain” of existing and approved blocks, using cryptographic signatures. Each new block has a time stamp corresponding to the development of new and permanent data – it contains the information on the preceding block, ensuring that each attempt to change it would require the changing of each of the blocks saved earlier⁶⁴. The authors of that definition indicate that that technology is extraordinary due to the possibility to ensure digital authenticity using cryptographic “evidence”. It is transparent and allows fast and cheap transmission of information and values in vast networks.

60 Sturta Habera, W. Scott Stornetta: How to time-stamp a digital document, *Journal of Cryptology*, 1991 No. 3 p. 99 et seq.

61 R. Anderson: *Security Engineering: A guide to Building Dependable Distributed Systems*, New York 2008, p. 5 et seq. See https://www.iacr.org/books/2010_ws_Anderson_SecurityEngineering.pdf of 11 marca 2018 and *Security Engineering: A guide to Building Dependable Distributed Systems 1st*. New York 2001, p. 6 et seq.

62 *Distributed Ledger Technology: beyond block chain*. A report by the UK Government Chief Scientific Adviser, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf of 23 June 2018.

63 Deloitte Australia: *Bitcoin, blockchain&distributed ledgers*” of 2016 r. p. 5.

64 E. Ducas, A. Wilner, *The security and financial implications of blockchain technologies*, pp. 544-545.

Two elements typical for blockchains were indicated by D. Maxwell, Ch. Speed, L. Pschetz⁶⁵ (Maxwell, Speed and Pschetz Larisa, 2017) : the first one is that it provides a response to the “missing link” of the digital system (allowing the introduction of “counterparts” of uncopiable digital goods that are verified and tracked in a network book (ledger)), and the second – that it is an undertaking characterized by (joint) participation.

Legal definition

Many states have demonstrated a very serious attitude to the subject and to the manner of using blockchains, as visible in the latest legal regulations associated with or containing definitions of blockchains or distributed ledgers. Act HB2417 was adopted in the State of Arizona (USA)⁶⁶ on electronic transactions. Blockchain technology is the subject of art. 5 which provides a definition of “blockchain” technology and specifies some of the consequences of using it.

"Blockchain technology" means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto-economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth.

The very innovative element is considering a signature secured by blockchain technology to be a signature meeting the requirements of an electronic form, and considering a document or contract secured by blockchain technology to be a document or contract in electronic form⁶⁷. Art. 5 allows smart contracts to be used in business dealings. Therefore, it will be impossible to dismiss the effects of a contract solely for the reason that it has been concluded as a smart contract. Furthermore, regardless of other regulations, it is considered that the data secured using blockchain technology is equivalent to other data, secured in other ways. That principle applies to ownership-transfer contracts or contracts for use.

65 D. Maxwell, Ch. Speed, L. Pschetz: Story Blocks: Reimagining narrative through the blockchain, *The International Journal of Reserch into New Media Technologies*, No. 23 (1) 2017r. p. 82.

66 <https://legiscan.com/AZ/text/HB2417/id/1497439>.

67 By the way – a very practical differentiation between documents (as carriers of any contents) in electronic form and electronic agreements.

In 2016, the state of Vermont changed the 12th title of the statute of Vermont – judicial procedure (chapter 81), entering, in § 1913, the definition and presumptions related to blockchain technology. In 12 V.S.A. § 1913 “Blockchain” means a cryptographically secured, chronological, and decentralized consensus ledger or consensus database, maintained via Internet interaction, peer-to-peer network, or other interaction. Information in digital form recorded in a block of chains is consistent with the legal presumption described in the Vermont Rule of Evidence 902, if it is connected to a written declaration by a qualified entity authorized to make certifications if it contains: the date and time in which the record entered the blockchain, the date and time of receipt of a record from the blockchain, the confirmation that the record was maintained in the blockchain as regular activity and that it was made by an entity that conducts such activity on a regular basis (recording using blockchain technology – author’s note). It is presumed (§ 1913 point 3) that a fact or record verified by correct application of blockchain technology is authentic. The date and time of a fact record or a record made using a blockchain is the date and time when the fact or record were added to the blockchain. The person performing the act using the blockchain is the registering person (a registered user). If parties agree on a specific manner of blockchain verification before a court or another tribunal, that confirmation, in the format specified by the parties, will constitute evidence. In the case of facts or data secured using blockchain technology, the burden of proof that the fact recorded using that technology or that the data, recording, time or identity of an entity are not authentic (as regards what was stated on the date of adding it to a blockchain), rests with the person making that claim. The presumptions resulting from that chapter apply, without limitation, to the facts and records made using blockchain technology for the purpose of determining: 1) the parties to a contract, its contents, effective date, status; 2) the ownership, assignment, negotiation and transfers of money and other legal instruments; 3) the identity, participation and status in creation, management of any entity (among others – legal persons – author’s note); 4) the authentic or integral character of a record, regardless of whether it is public or private information; 5) the authentic or integral character of communication records. At the same time, it was clearly specified that the records, acts or information recorded using blockchain technology may not be dis-

missed⁶⁸. On 30 May 2018, the S. 269 Act Related to Blockchain Business Development was adopted, in which the blockchain definition included in 12 V.S.A. was repeated and the following additional definition was introduced: ““Blockchain technology” means computer software or hardware or collections of computer software or hardware, or both, that utilize or enable a blockchain.

In Europe, one of the areas that introduced the definition of distributed ledgers is Gibraltar. Its Financial Services Regulations 2017 of 12 September 2017 (effective from 1 January 2018)⁶⁹, did not define a blockchain, but rather DLT – point 10 defines a distributed ledger or DLT as a system of databases, in which data and information is recorded, shared and synchronized in a network of nodes, and all the database files are treated as equally authentic.

On 21 December 2017, the President of Belarus issued decree No. 8 on the development of the digital economy (effective from 1 January 2018). The decree specifies the general principles of functioning of the digital economy in Belarus and opens the economy to foreign technologies, including IT specialists (among other details, they do need a visa or a work permit). The operations of cryptocurrency exchanges and trading in tokens were formally allowed, and appendix No. 2 to the decree introduced new terms, including the following definition: Transaction block ledger (blockchain) – a sequence of blocks with information about operations performed in such a system built on the basis of given algorithms in a distributed decentralized information system using cryptographic methods of information protection⁷⁰. An interesting addition, unseen in other states, was the introduction, in legal regulations, of the definition of (mining) related to blockchains. The regulation introduced and functioning from 1 January 2018 is very modern and meets the needs of participants in the digital economy (including, for the purpose of settlements, that an operator

68 The change of law led to the development of companies, the activity of which is based on blockchains. What is interesting is the first transaction with a notarial deed recorded using blockchain technology was conducted on 8 March 2018 in Vermont. <https://cointelegraph.com/news/vermonts-pilot-program-completes-first-us-all-blockchain-real-estate-transaction> of 9 November 2018.

69 Gibraltar Gazette, No 4401. [http://www.gfsc.gi/uploads/DLT%20regulations%20121017%20\(2\).pdf](http://www.gfsc.gi/uploads/DLT%20regulations%20121017%20(2).pdf) of 23 June 2018.

70 <http://law.by/document/?guid=3871&p0=Pd1700008e>.

of a cryptographic platform may open accounts in banks outside Belarus as well as establish virtual wallets, and transfer tokens abroad)⁷¹.

The above review of definitions of the term 'blockchain', both from the points of view of the doctrine and of the law (the results of last months' legislation), provide a picture of more and more frequent acknowledgment of that technology and of undertaking the activities aimed at supporting the development of the digital economy. It would be impossible without the proper legal framework, and without properly defining the new terms.

The definitions presented above demonstrate several repeating elements: a distributed ledger, with a continuous increase in records, verified and grouped in blocks, secured cryptographically. In other words, it is a sequence of blocks with information on the operations performed in the system constructed on the basis of algorithms recorded in a distributed, decentralized IT system using cryptographic methods of information protection.

Blocks

Blockchain technology uses so-called blocks, differently from classical DLT, which is a component of blockchain technology⁷² (Maxwell, Speed and Psetz, Reimagining narrative through the blockchain, 2017). It consists of a heading and data (transactions).

The heading contains a reference to the preceding block in the chain (the so-called hash), then a time stamp that specifically indicates the time of establishment and the so-called merkle tree root of all transactions included in the block⁷³ (Roth, 2015).

The same data block contains 1) the merkle tree root of all the transactions included in the block and 2) the transactions of the given block⁷⁴ (Piech, 2018).

Such classification is very practical and significantly accelerates searching for data. As a single block may not contain too much data, and its mul-

71 A tax exemption (income tax, VAT, profit tax, etc.) was introduced for Residents of the New Technology Park established with a decree, until 1 January 2023.

72 D. Maxwell, Ch. Speed, L. Psetz, Story Blocks: Reimagining narrative through the blockchain, [in:] *The International Journal of Research into New Media Technologies* 2017 No. 23 p. 79 et seq.

73 N. Roth: An Architectural Assessment of Bitcoin. Using the System Modeling Language, *Procedia Computer Science* 44 (2015), p. 530.

74 K. Piech *Leksykon*, 2018, p. 5.

title is included in the chain, the time required for searching everything, even using very strong computers or networks thereof, might be very long. Inclusion of a hash in a heading allows for searching for transactions by their hashes, without the need to read out all the data included in the blockchain. In a search, only the headings and merkle tree roots are read automatically, without the physical participation of a person. That practice is not different from the previous searches for documents or for information or data contained in traditional registers. A heading and the data (from the block) included therein may be compared to a list of contents and (page) references in a traditional register. The difference is between full automaticity in blockchains and a physical search by a person in a traditional register (be it electronic or paper).

Hash is a short combination of characters assigned to a dataset of any size using a hash function. In blockchain technology, it is important that it is resistant to double generation of the same hash to different datasets and that it is unidirectional, i.e., that it is impossible to obtain the data based on the hash value itself⁷⁵. The hash function has been successfully used for many years in PKI in the scope of qualified electronic signatures, time stamps and qualified electronic stamps, wherever it is required to guarantee authenticity and integrity of signed data and, as a result, its confidentiality and non-repudiation.

A blockchain contains the full history of a transaction, available to everyone and stored by everyone. The transaction is grouped in blocks. The number of transactions depends on the size of the data. The limit for a block may be different, e.g., in Bitcoin it is 1,000,000 bytes. The heading consists of seven fields, while the block version number depends on the version of the software used for generating it. The SHA256 hash of a heading must be lower than or equal to the calculated current hash (the so-called mathematical problem to be calculated by the miners) for the block to be accepted. The number of transactions included in the block is displayed in the heading field⁷⁶ (Bhaskar and Kuo Chuen, 2015).

75 K. Piech: *Leksykon*, 2018, p. 12.

76 Bhaskar, Nirupama Devi; Kuo Chuen, David Lee: *Bitcoin Mining Technology*, [in:] *Handbook of Digital Currency*, ed. Kuo Chuen, David Lee, Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo 2015, p. 48.

Consensus

In the Bitcoin blockchain, the whole block must be cryptographically signed by “miners”, which may be treated as “taking up a cryptographic shield” that guarantees that the data on transactions will not be altered. The closing of a block creates a new link of the distributed chain, ready for recording further transactions.

The signing takes place using many different consensus algorithms, and so there are many technologically different blockchains, e.g., Proof of Work (PoW) or Proof of Stake (PoS), etc.

Proof of work is a mathematical operation, the result of which is very easy to verify from the outside (e.g., by entering a calculated variable in an equation), while the very generation of the result requires a gigantic number of mathematical calculations (the algorithm selects a mathematical problem so that its calculation time is permanent regardless of the computing power of computers)⁷⁷. The calculation is performed by multiple “miners” and multiple devices (diggers). You never know which will be the first one to calculate the PoW correctly, and so to generate (sign) the next new block, because the problem's solution has a random value (searched for by trial and error). The computing power required for correct calculation is different depending on the type of blockchain. In Bitcoin, it is gigantic, which currently guarantees the cybernetic security of a signed block (computing power of the same size would be required to overcome the security mechanisms). As “the security of integrity of the whole data chain of a distributed ledger is that each block refers to the preceding one, i.e., contains a chain of data based on the results of successive calculation results from preceding blocks, generated using gigantic computing power”, for it to be breached in Bitcoin would require a level of computing power that is currently impossible to obtain. As the blockchain continues to grow continuously, even in the case of doubling the computational capacity of the current processors, the calculated blockchain secured with the respective cal-

77 M. Grzybowski, Sz. Bentyn: *Kryptowaluty*, p. 35. They indicate that the basic difficulty with calculating the PoW is imposing the value of the first character that has to include the solution, so as to be able to calculate the correct hash function in the SHA256 algorithm. Additionally, Bitcoin algorithms impose a suitable number of zeroes at the beginning, depending on the difficulty of the calculation. The Bitcoin algorithm is structured so that, regardless of the computing power of the computers calculating the hash, it always takes ca. 10 minutes. In case of need, the algorithm increases or decreases difficulty of the problem by adding or removing a suitable number of zeroes at the beginning.

culations using the increased computing power would continue to be secure in cybernetic terms. An increase in the computing power spent on PoW causes the security of the approved transactions to improve. In turn, in blockchains (particularly private ones), in which gigantic computing power is not applied, the value of non-repudiation is much lower.

PoW as an algorithm “looks after” the reaching of a *consensus*, or “the process within which the parties taking part in a network based on blockchain technology agree to conduct a transaction approved by all the participants in the network⁷⁸” or by the entities authorized to approve it (e.g., ledger operators). PoW is an algorithm used for acceptance of and approval for Bitcoin blockchains, among others.

Other ways of reaching consensus indicated in the literature⁷⁹ (Piech K., 2017) include:

Proof-of-Stake (PoS) a “method based on the amount of currency possessed. The more units of the given currency a participant has, the bigger the chance that it will establish a block⁸⁰”. A little broader definition was indicated by V. Morabito (Morabito, 2017) – he stated that PoS is an alternative to PoW, and proof and consensus do not require such costly calculations as PoW. PoS depends on the participation by entities within the given holding. A block is confirmed and established by whoever has a greater share⁸¹.

“*Delegated Proof-of-Stake* is based on selection, by currency owners, of certain delegates who are authorized to add new blocks to the blockchain;

Provable Data Possession (PDP) allows users to send data to the given server and then to verify the data stored there;

Proof-of-Storage – ordering another user to store data, and then verifying multiple times whether it is still stored.”⁸²

Other methods are derivatives of the following examples, often hybrids of Proof-of-Work and Proof-of-Stake.⁸³

78 K. Piech, Leksykon, 2018, p. 8.

79 K. Piech (ed.) Podstawy korzystania z walut cyfrowych, Warsaw 2017, p. 22.

80 K. Piech (ed.) Podstawy p. 22.

81 V. Morabito: Business Innovation Through Blockchain, Cham (Springer) 2017, p. 11.

82 K. Piech (ed.) Podstawy, 2017, p. 22.

83 V. Morabito: Business Innovation Trough Blockchain, p. 12.

How does it work?

In order to explain the principle of blockchain technology, we should examine the traditional ways of maintaining ledgers. Since the dawn of time, business dealings, in particular circulation of goods, values, etc., have been based on recording of facts (sometimes whole documents) for evidentiary purposes, in particular for demonstrating the rights entered in the ledger. Ledgers are maintained by the so-called trusted entities – established, functioning and controlled in accordance with proper legal regulations (e.g., banks maintaining the accounts, courts maintaining the trade registers, land and mortgage registers, etc., accountants keeping accounting books). These registers, as indicated before in discussion of DLT, are usually centralized, and in trading there appears an intermediary trusted by all the users, with full control over the system, who assists in transactions⁸⁴. In practice, the users (e.g., bank clients) do not directly control the entries (in the system), but may only exercise follow-up control and raise claims in the case of violation of laws or occurrence of liability for damages. The data and base are centralized (having nothing more than backups). However, apart from access to that base, a user does not have a “copy” thereof. This means that, in practice, in the case of a banking-system failure, the persons holding bank accounts may not prove their rights or the fact of performing, for example, a banking act, or it is highly difficult.

Before the stage of informatization (e.g., in 1980s or earlier), the register maintained in an institution was accompanied by “home registers” of the users (e.g. account owners) in the form of accounts books, savings books, copies of proofs of payment, etc.

DLT technology, including blockchain technology, offers the same functions as centralized registers, by providing users with a base or a part associated with them (depending on the types of keys available), modeled after the previous “home registers”, because their architecture is not centralized, and each participant has its “copy”, or actually its part of the register, identical to that of others (which means that everyone has access to all the data included therein, which may be cryptographically limited). Everyone may request the adding of any transaction to the blockchain, but transactions are only accepted when the users authorized to perform such a transaction consent to it. For example, in the case of payment under a sales agreement,

84 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf of 25 June 2018 p. 5.

to record a transaction, what might be necessary is acceptance by the seller (confirming, among others, its account and the fact that it is transferring the ownership of a thing) and by the buyer (that it purchases that thing and pays for it (today, in practice, when transferring money, the beneficiary does not have to consent to anything, and there are frequent mistakes in account numbers)). The process of verification and consent is performed fully automatically (today, when using electronic banking, everything is fully automatic on the part of the bank). Transactions are performed by many users of the system at the same time, and these transactions (after approval, naturally) are joined and registered in blocks and cryptographically secured by the so-called miners (as there are many transactions, they wait for “their turn” to become joined in a block). If someone is in a hurry, they may “purchase” priority of entering the given transaction in a block, by declaring the amount of commission to be obtained by the miners at the given transaction. In order to imagine that process, we may compare the respective blocks to a sheet of paper, on which many participants enter their transactions (e.g., declarations by the seller and buyer), everyone enters their transaction and signs it, thus authorizing the previous transactions on the sheet, until there is no more space. Then, a list of contents is generated with a reference of where the given declaration is (i.e., a heading and hash tree root are generated). When the sheet is complete, it is secured (e.g., with a stamp) and another one is started which, after being filled in, is attached to the previous sheet (e.g., glued together) and joined to it, e.g., with a signature and impression of a stamp on the borderline between the sheets. An identical activity takes place in a blockchain, by adding a link to a chain of transactions and securing it. The chain makes up the ledger, to which all the users are entitled⁸⁵ (Khan, 2015/maj) (and have a “copy” thereof saved on their devices, or rather an identical, integral and cohesive part of the ledger). Such activity is called mining. Additionally, on the network computers (so-called diggers), there is simultaneously being solved a complicated mathematical problem consisting of generating a properly encrypted block of transactions (proof of work) which is added to the blockchain (thus guaranteeing cryptographic security). It is as if, on a traditional sheet, the best artists prepared a complicated drawing, the best of which (and consistent with the problem visible on the sheet) is placed on

85 A. Khan: Bitcoin – payment method or fraud prevention tool? ; Computer Fraud & Security May 2015, p. 18.

it as additional security, so that the sheet may not be forged⁸⁶. Adding another block to the chain means updating the lodger of all the users, including previous ones. Acceptance of a block takes place only when the transactions included therein are verified. If there are discrepancies, the block is rejected. The chain generated in that manner is very difficult to alter, and currently practically impossible taking into account the large computing power of the participating computers. It would also be very difficult, or even impossible, to destroy it, because there are as many “copies”, or actually identical ledgers, as there are users, and destroying a ledger would require a simultaneous and effective attack on all the “counterparts”. Also, it is impossible to have a “false register”, because every user has their own, true version which may be compared with others⁸⁷. Just like before the era of digitization, “home” documents could be compared with others, e.g., from a bank (although at that time it was not one distributed ledger, but rather distributed documents).

The above-mentioned model of operation of the blockchain technology, and also of miners, has already been included in the provisions of the above-mentioned Decree No. 8 by the President of Belarus of 21 December 2017, regarding development of digital economy.

Appendix No. 2: “Mining – activity different from the creation of own digital signs (tokens), aimed at ensuring the functioning of the transaction block ledger (blockchain) by means of creating in such ledger of new blocks with information about performed operations. A person carrying out mining becomes the owner of digital signs (tokens) arisen (mined) as a result of his activity on mining and can receive digital signs (tokens) as remuneration for verification of the performance of operations in the transaction block ledger (blockchain).”⁸⁸

86 In practice, in order to solve the problem, you need very large computing power. And the miner (computer) that first solves the complicated problem will receive the remuneration. There are different ways of rewarding miners for calculations. These may include, for example, a commission on the value of the transaction. It is as if an artist received remuneration for drawing the most complicated picture on a sheet of paper (in order to secure it).

87 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf of 25 June 2018. p. 5.

88 <http://law.by/document/?guid=3871&p0=Pd1700008e> of 12 November 2018.

Types of blockchains

Blockchain technology may be applied in different ways. There are three basic types of blockchains: public, private and hybrid⁸⁹. The best-known and revolutionary one is a public blockchain, mainly for the reason that it is the foundation for Bitcoin. A public blockchain is fully open-source, within which everyone, without any personal or territorial limitation, may install suitable software their own device and download the whole or any fragment of a database and, usually (like in the case of Bitcoin), make its “copy” available to other nodes. Operations within private blockchains usually do not require the consent of the ledger operators. What is needed is consensus from the users. Public ledgers, such as Bitcoin, do not have one “owner” and are resistant to censorship, which means no one can block the entering of a transaction in the ledger⁹⁰.

From a technical standpoint, a private blockchain is based on the same technology of connecting chains in blocks as a public blockchain. However, it is not available for everyone. In this case, a blockchain may be downloaded or provided only by a specific group of entities. “A private blockchain is used when a business network contains confidential data or when legal regulations do not allow the respective users to use a public blockchain”⁹¹, and operations in a ledger require authorization by ledger operators. The possibility for the given person to use a private blockchain usually results from an agreement concluded either with the software licensor or among the users themselves (e.g., within a consortium) or from the legal regulations specifying the access rights of the respective users. A private blockchain is usually (but not only) used in projects and agreements of a gainful character.

The last type is the theoretical example of a hybrid blockchain that functions as a private network with its own consensus protocol and ledger-access control mechanisms, but uses a public blockchain for settlement purposes and for confirming the existence of the given condition at the given time (proof of existence) or to use cryptocurrencies.

According to another criterion, blockchains may be divided into a blockchain provided to network users with prior consent (e.g., of the ledger operator or another entity), i.e., the so-called *permissioned blockchain*

89 V. Morabito: Business Innovation Through Blockchain, p. 8.

90 <http://fintechpoland.com/wp-content/uploads/2017/01/Technologie-rozproszonych-rejestrow-UK-GOfS-FTP-NASK-PL-1.pdf> p. 13.

91 K. Piech: Leksykon, 2018, p. 6.

or a *permissionless blockchain, provided to anyone*. The former is used in business, or corporate, solutions, or by state authorities, while the latter – e.g., in Bitcoin.

Another classification is into *immutable blockchains* and *editable blockchains*⁹². An example of the former is the Bitcoin blockchain, where you may only add information and may not correct it, and the computing power guarantees its security. An editable blockchain allows interference with historical data by authorized entities, i.e., a ledger operator that is, in practice, a trusted third party.

It seems that blockchains may also be classified from the point of view of the method of block management. It may either be managed in a decentralized way through democratic consensus, one example of which is the Bitcoin blockchain – managed by a majority of users through consensus, or a blockchain managed by a ledger operator (e.g., by a bank corporation, state authorities using blockchains, etc.).

92 Classification presented by K. Piech: Leksykon.

Chapter III. Blockchains in finance⁹³

Introduction

Distributed ledger technology (DLT), as well as blockchains, are usually associated with the appearance of cryptocurrencies, in particular Bitcoin. Currently, it is used for various purposes, but the first and most serious implementations were associated with cryptocurrencies.

The concepts of using cryptography in financial transactions and payments appeared much earlier than cryptocurrencies. In the 1980s⁹⁴ (Chaum, 1985) and 1990s, many publications on cryptography, mathematics or IT, included a number of comprehensive cryptographic solutions describing new payment systems possible to implement in finance⁹⁵. These were innovative solutions⁹⁶ (Eodel, 1997), describing cryptographic protocols, exceeding the previous understanding of cryptography known in the world of banks (Roth N. , 2015 nr 44). The main discussion and suggested solutions were associated with implementation of electronic money⁹⁷, including whether it should function in transactions anonymously⁹⁸, (Law, Sabett and Solinas, 1997) or under control. The concept of development of electronic money and its extensive, anonymous use similarly to the use of

93 The purpose of this chapter is not to present tokenization and patterns of using cryptocurrencies. That issue is so broad that it should be covered by a separate monograph. This chapter presents certain aspects of using blockchains in finance.

94 D. Chaum: Security without identification: transaction systems to make Big Brother obsolete, [in:] Communications of the ACM, No. 10/ 1985 p. 1030 et seq.

95 An important stem in development of cryptocurrencies was development by Adam Back, in 1997, of the hashcash proof of work (PoW) function which was applied by Hal Finney for developing a reusable proof of work (RPOW) which was used by B. Money, and then by Nick Szabo for the Bit Gold project. See also N. Roth: An Architectural Assessment of Bitcoin [in:] Procedia Computer Science No. 44 (2015) p. 528.

96 D. G. Oedel; Why Regulate Cybermoney, [in:] The American University Law Review No. 46 of 1997r. p. 1075 et seq.

97 Piotr Rutkowski: Pieniądze usieciowione [in] Raport Wirtualne waluty, Wardynski i Wspólnicy, Warsaw 2014, p. 6. http://www.wardynski.com.pl/w_publication/wirtualne-waluty/ of 5 July 2018.

98 L. Law, S. Sabet, J. Solinas: How to make cryptography of anonymous electronic cash, [in] The American University Law Review No. 46/ 1997, p. 1131 et seq.

regular cash, were not developed or implemented by financial institutions as a result of the attacks on the World Trade Center of 11 September 2001. Development of new technologies, globalization of the economy, openness of markets, including ease of concluding online agreements, as well as ease of delivering goods abroad (a good example of which is the Chinese portal Alibaba, which delivers goods to the value of hundreds of millions of dollars to almost every place in the world), as well as the appearance of the digital economy, with relatively high costs of payments, had to lead to the generation of alternative, cheap and global methods of payment. A lack of proper activity by banking institutions which, it seems, failed to notice the needs of the global digital economy, and relied on technological development of previous payment methods (also based on cryptography) resulted in the appearance of “private money” and the concept of using it for online payments. The implemented concept of Bitcoin, published by an anonymous author or authors under the nickname of Satoshi Nakamoto⁹⁹, is a good example. And the blockchain technology applied in that concept turned out to be a revolutionary IT tool.

Globalization, including the global economy, are becoming real. This does not mean the end of the previous economies or manners of functioning of states, including regulators. However, it forces a new approach and the need to accept new tools or institutions functioning in the digital economy which, often at least in the preliminary stage, seem diametrically different from the previous ones, while in fact they only constitute an evolutionary element of development of the previous concepts.

Examples include blockchains and cryptocurrencies, at first negated and perceived as infringing upon the previous legal or social order, rejected by a number of institutions or experts¹⁰⁰. The next stages were “familiarity” and acceptance (right now that stage is at a different level in different states or institutions), and the attempts at regulation in different areas of the law (including tax law, financial law and civil law), as visible in the latest legislation, defining cryptocurrencies, blockchains and trading in them. The statement by Milton Friedman from 1960 is characteristic: “the moderately stable monetary framework seems to be the necessary condition for effective functioning of a private market-based economy. It is doubtful whether the market itself may provide such a framework. As a result, the function

99 <https://bitcoin.org/bitcoin.pdf> of 5 July 2018.

100 Within the meaning of negation of technology and of the potential benefits of applying it. Not to deny the correctness of the warnings about the value of Bitcoin and about the risk associated with trading in it.

of provision is the basic governing function, together with provision of a stable legal framework¹⁰¹” (Friedman, 1960).

Blockchains in financial institutions

In 2012, the European Central Bank published its first report on virtual-currency schemes¹⁰² resulting from an analysis of 2011. It indicated the direction of changes and the positive aspects of technological and financial innovations aimed at providing consumers additional, alternative payment methods. It was also mentioned that the share of consumers in those systems exposes them to risk and it is necessary to observe the market.

The 2015 report¹⁰³ included a number of warnings and emphasized that cryptocurrency is not money in a traditional sense and, despite the existence of different types of cryptocurrencies, it does not pose a risk to the global financial system. At the same time, EBC admits that, apart from drawbacks, the use of blockchain technology and the creation of virtual “money” may also have certain advantages in comparison with traditional payment solutions, in particular with regard to payments in virtual community environments/closed subscription loops or cross-border payments. As a result, it is possible that in the future a new or improved system will be beneficial for the financial sector¹⁰⁴. Direct or indirect regulatory activity is becoming necessary. For them to be efficient, they have to be developed at an international level.

EBC is not the only entity analyzing the new technology. For example, the World Economic Forum and GFC (26) established the group called The Future of Blockchain as one of thirty-five so-called *Global Future Councils* for the purpose of analyzing the new technology and its practical applications. The largest banks in the world have established consortia for the purpose of supporting their activity in the scope of research, but also of supporting the consortium members, noting the actual benefits for the industry and streamlining of processes. However, the issue of proper security, including of documents and financial processes, in banking is significant.

101 Friedman, M. (1960), *A Program for Monetary Stability*, New York: Fordham University Press p. 7 et seq.

102 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> of 14 May 2018.

103 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>.

104 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>.

For illustrative purposes only, because practically all the key banks and financial institutions conduct, to a higher or lower degree, research, studies or implementations aimed at applying blockchain technology, one may indicate the consortium of the following banks J.P. Morgan, Royal Bank of Scotland, Credit Suisse, Goldman Sachs, etc., making up the R3CEV's consortium (aimed at designing and delivering advanced blockchain technologies for global financial markets). Another example is the Canadian consortium of Bank of Canada, Payments Canada and R3 aimed at introducing blockchains in the financial infrastructure of Canada, or the practical implementation of blockchains by National Bank of Canada and Canadian Imperial Bank of Commerce in cooperation with ATB Financial – enlisting the services of San Francisco-based Ripple Labs. Another example is State Bank of India (SBI), which established¹⁰⁵ a consortium consisting of 27 banks of India (BankChain) and technological companies (among others Microsoft, Intel and IBM) piloting the project of applying smart contracts in domestic banking (for simple agreements) and 9 other projects (including factoring, document circulation and ledgers). A successful implementation (May 2017) based on DLT is the Know your customer (KYC) platform called ClearChain, allowing banks to provide data on their clients within the consortium (including information and reports on suspicious activity)¹⁰⁶.

Other examples include a consortium of Russian banks or the activity of Spanish Santander (Fintech 2.0 document and proposed solutions). There are a number of reports indicating savings for the financial sector on account of blockchains (which in 2022 may amount to as much as ca. USD 15-20 billion) (Wielens, 2016). CitiGrop is testing its digital currency (Citi-coin) and UniCredit is analyzing blockchain-based payments¹⁰⁷ (Biella and Zinetti, 2016).

In Germany¹⁰⁸, a number of licensed banking institutions are being established, the activities of which are blockchain-based. An example is So-

105 8 February 2017.

106 See www.bankchaintech.com.

107 M. Biella, V. Zinetti, *Blockchain Technology and Applications from a Financial Perspective*. Technical Report Version 1.0, UniCredit, 26 February 2016r, p. 3 et seq. <https://www.weusecoins.com/assets/pdf/library/UNICREDIT%20-%20Blockchain-Technology-and-Applications-from-a-Financial-Perspective.pdf> of 11 November 2018.

108 Over 1300 programming projects related to blockchain technology appeared in Germany before the end of 2018.

larisBank¹⁰⁹, which provided, for its clients, the so-called “corporate blockchain accounts” which, however, may only be opened in fiduciary currencies, and also allows the purchasing and selling of state currencies using cryptocurrencies. In 2018, in cooperation with SolarisBank, VPE Wertpapierhandles Bank AG (German Securities Investment Bank, established in 1989) allowed its clients to purchase cryptocurrencies, with its activities in that regard being based on blockchains.

A similar pilot program (spring 2018) was conducted by the German licensed financial institution Bitbond which replaced the previously used SWIFT system with cryptocurrencies and blockchain technology for international settlements (exchange of resources with FIAT guarantee of amount)¹¹⁰.

In June 2018, an experiment was conducted in Germany using the Know Your Customer (KYC) system by R3 to conduct 300 international transactions in 19 countries among 39 entities, using R3 blockchains. What is important is that the tested entities included the following banks: BNP Paribas, Deutsche Bank, ING, Raiffeisen Bank and Sociate Generale. The experiment also covered the Federal Reserve Bank in Boston, the Central Bank of Colombia and a financial regulator from Peru¹¹¹.

The above indicates a significant trend of using the blockchain technology in the financial sector, started by the appearance of Bitcoin. However, the Bitcoin blockchain is not the only tool used by financial institutions.

Bitcoin¹¹² and its Bitcoin blockchain

For the first time, a blockchain was used in practice to create the Bitcoin cryptocurrency, as an element of Bitcoin software¹¹³. This does not mean, however, that it is solely connected to that cryptocurrency. It constitutes a

109 <https://www.solarisbank.com/en/>.

110 <https://www.digitalassets.pl/ten-niemiecki-bank-preferuje-bitcoin-zamiast-swift-dla-miedzynarodowych-transferow/>.

111 <https://bithub.pl/wiadomosci/blockchain-r3-przetestowalo-juz-39-firm-w-tyming-i-deutsche-bank/>.

112 The purpose of this study is not to analyze the legal aspects of Bitcoin, just to indicate the legal issues associated with using blockchains. The legal status of Bitcoin is so broad that it deserves a separate publication.

113 In this study, the word “bitcoin”, starting with lower case “b”, refers to the cryptocurrency, while the “Bitcoin software”, starting with upper case “B”, refers to the software.

certain kind of data recording in blocks, and may take different forms depending on software and, in particular, on the manner of reaching consensus. The blockchain applied in Bitcoin software and used as the data authorization tool, is only one type of blockchain. Currently, it provides the highest degree of cybernetic security due to the computational capacity used for calculating PoW by “miners” (hereinafter referred to as the Bitcoin blockchain).

Bitcoin – how does its blockchain work?

The first entry in the Bitcoin blockchain was made on 9 January 2009, probably by Satoshi Nakamotoi, and informs of the fact that the holder of the given public address ¹¹⁴ (which might be compared to a bank account number) 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfN generated the first 50 bitcoins¹¹⁵. It was the beginning of the ledger of blocks, and each subsequent entry referred to the first entry, recorded in the first block and in the future blocks generated since. Each newly generated bitcoin is entered in a block, with information on what address it has been assigned. As a result, the block ledger contains the entries of all the information on the generated bitcoins and on the addresses to which they have been assigned, starting from the first 50 bitcoins. Each bitcoin has a unique number and is divisible into 100,000,000 units called satoshi (just like dollars or euros are divisible into cents, with the reservation that a dollar/euro has 100 cents, while one bitcoin is divisible into 100,000,000 units). Each unit has its own unique number¹¹⁶. In literature, satoshi are usually described as a fraction of a bitcoin, e.g., BTC 0.00035. The Bitcoin blockchain gains not only the information on the newly created bitcoins, but also on all the transfers related thereto. It is as if, in the case of dollars or euros, every transaction using the given banknote (e.g., a store purchase, donation, etc.) were recorded in a ledger. As the ledger of the Bitcoin blockchain is public, everyone

114 A so-called wallet.

115 D. Yermarck: *Is Bitcoin a Real Currency?*, p. 34.

116 Just like every banknote issued by the State has a unique number. In the case of a blockchain, the smaller units have individual numbers also, which is not the case for coins in the real world (being equivalents of satoshi). See *Podstawy korzystania z kryptowalut*, ed. K. Piech, Warsaw 2017, p. 15, in a note referring to prof. dr hab. Marian Srebný.

may check what transactions¹¹⁷ were performed using every bitcoin or its satoshi, as well as what bitcoins were situated in the given wallet and when, and what transactions were performed using the given wallet¹¹⁸. The entries in the book are publicly available, including wallet numbers (just like bank account numbers, the difference being that, in a bank account, third parties are not able to verify the transactions performed, while in the Bitcoin blockchain software anyone may enter and check each wallet number). In turn, the persons being the holders of the respective wallets function in the blockchain on an anonymous basis. What is important is the global scale, i.e., anyone in the world may open a wallet and make Bitcoin transfers using the Bitcoin blockchain (e.g., by making transactions under a contract concluded before).

Each transaction is recorded in a block, the size of which is permanent and currently amounts to 1 MB (1,000,000 bites). Each new block is connected to the previous ones, which means a continuous increase in the size of the Bitcoin blockchain book (at the moment of writing this monograph, it amounted to 204.42 GB, and two days later – 204.7 GB)¹¹⁹ and continues to rise as a result of the newly recorded blocks¹²⁰. The new entries, or rather the computational capacity used for generating blocks, and the cryptography recorded in them, currently guarantee permanence of entries. The essence of Bitcoin is that entries are continuous and blocks expand continuously, every 10 minutes, to be exact.

117 The first historical “transaction” using Bitcoin was performed by a programmer from Florida, Laszlo Hanyecz, who bought two pizzas for 10,000 bitcoins. In practice, he did not pay with bitcoins, but used his credit card to pay, for a transfer of 10 bitcoins to his wallet, to their previous holder. The first “actual” payment using Bitcoin was acceptance by a farmer from Massachusetts, David Forest, of Bitcoin as payment for alpaca juice. See B. Wallece: The rise and fall of Bitcoin, www.wired.com/2011/11/mf-bitcoin/ ; see also D. Yermack, *Is Bitcoin a Real Currency?*, p. 35.

118 Just enter one of the “Blockchain Explorer” websites, e.g., for Bitcoin – blockchain.info, where you can trace the current, and also historical, transactions. Just type the *block number*, *address*, *block hash*, *transaction hash*, *hash160* or *ipv 4 address*.

119 <https://bitinfocharts.com/pl/bitcoin/> of 7 July 2018.

120 530,840 blocks existed on 7 July 2018 at 8:27:56.

The size of each block was determined in the blockchain software, but may be amended on the basis of so-called consensus¹²¹ in case of need¹²². That size is significant for the speed of recording the transfers among wallets. Every entry includes data of a certain size (on average, one entry in the Bitcoin blockchain amounts to a little more than 500 bytes). A block may include no more than 1 MB of data, which means that no more than 2,000 entries may be made in one block. Subsequent entries are made in the next generated block. Blocks are calculated (generated) by miners who calculate the cryptographic value of a block by signing it cryptographically at the same time all over the world, each with access to the whole blockchain ledger and waiting for subsequent entry shifts in the block. In practice, every shift between wallets is “signed” by several or even about a dozen miners all over the world (after transaction verification and validation). The Bitcoin blockchain algorithm is constructed so that the calculation of every block (recording a transaction in a block) takes ca. 10 minutes. This means that no more than 2,000 transactions may be recorded every 10 minutes, no more than 12,000 every hour and no more than 288,000 shifts between wallets may take place during a day, in 6 blocks per hour and 154 per day.

That form of recording, with the initial low interest in Bitcoin, guaranteed fast shifts and fast entries in the book. Currently, on account of the significantly growing number of transactions¹²³, recording a transaction may take up to several hours. A shift consists of indicating the wallet (its number) to which the shift is to be made (like a transfer to a bank account) – the transferred bitcoin is shifted to the so-called Meempool (from Memory Pool) and then the bitcoin “disappears” from the transferring wallet, and only “appears” in the target wallet after the transaction is recorded in the Bitcoin block. As indicated above, that is not even instantaneous, unless the person waiting for an entry in the block to be made “purchases” priority of entry – then the entry may be made in the next recorded block, i.e., every 10 minutes. Entry priority may be purchased from miners, by offering payment via the websites used for transferring Bitcoins. For example, on 11 July 2018 the average fee for “quicker” entry in a block amount-

121 Satoshi Nakamoto indicated in Bitcoin. A Peer-to Per ..., that the size of a heading of a block without a transaction should be 80 bytes, which results in 4.2 MB per year. <https://nakamotoinstitute.org/bitcoin/> of 11 July 2018.

122 The Bitcoin Cash cryptocurrency (the 4th cryptocurrency in the world in terms of capitalization) appeared as an alternative to Bitcoin, and offered an increased block of 32 MB.

123 193,917 per day and 8,080 per hour on 6-7 July 2018.

ed to 0.1298 BTC (Bitcoin) for a whole block which amounted to USD 877.18 at the then value of Bitcoin of USD 6,758 (11 July 2018).

Apart from the fee for making a “faster” entry in a block, the Bitcoin algorithm is constructed so that new bitcoins are generated every 10 minutes, which are assigned to one of the miners, who solves an extremely complicated cryptographic problem for the given block, whose problem also constitutes a mechanism of cybernetic security. The difficulty of the calculated problem rises together with the increase in the computing power, used for calculating it, of miners’ computers (so that the calculation is complete no sooner or later than in 10 minutes) which takes place after each 2016 blocks, i.e., after the lapse of ca. 14 days (system self-control)¹²⁴. The rising computing power of the computers used for calculating the problem secures the Bitcoin entry blocks better and better, adding one to the next. The new bitcoins are generated based on the following rules: 50 BTC was assigned for blocks 1 – 210,000. 10.5 million BTC was thus generated. For the next four years, half of that amount was signed, i.e., 25 BTC per block, thus generating another 5.25 million BTC. After 4 years, the assignment of bitcoins per block was decreased to 12.5 BTC until 2.625 BTC were generated (it’s the value of the current assignment), and in the next four-year period the assignment is going to decrease by half again, etc., until the generation of 21 million BTC, which will take place in 2140¹²⁵ (Bhaskar, *Bitcoin Mining Technology*, 2015). When this monograph was written, 12.5 BTC was assigned for a block, at the value of USD 84,450 per block¹²⁶.

A transaction is confirmed in the Bitcoin blockchain by reaching consensus (transactions are approved differently in different types of blockchains) which consists of verifying which transactions are correct and should be entered in the blockchain ledger. What is verified is whether the given bitcoin has actually been generated, assigned to the given person, etc. Everything takes place automatically in all the nodes calculating the

124 If it turns out that calculation of a problem in the last 2016 blocks takes more than 10 minutes – the system will adapt (the problem will become less difficult). No more than four times, however. MN. Grzybowski, Sz. Bantyn: *Kryptowaluty*, p. 37.

125 N. Roth: *An Architectural Assessment of Bitcoin*, p. 527 et seq.; N. D. Bhaskar: *Bitcoin Mining Technology* [in] *Handbook of Digital Currency*, ed. Lee Kuo Cheun, New York 2015 p. 46 et seq.

126 For that reason, many entities in the world perform cryptographic calculations hoping to generate bitcoins for themselves, while being cryptographically protected.

given block. In the Bitcoin blockchain, positive verification (verification with the previous blocks) must be positive in over 50 percent of nodes. That verification is validated using the Proof-of-Work protocol¹²⁷. It is very easy to verify it, while generating it requires a gigantic number of attempts¹²⁸.

Bitcoin blockchains – legal issues

Introduction

The issue of Bitcoin is not only the issue of an innovative, highly advanced technology, but, in particular, entails a number of legal problems and questions regarding the character of Bitcoin itself, its creation, miners' work, Bitcoin-transfer approvals (transactions), trade in bitcoins, or relationships among the respective entities participating in the mining process. One of the fundamental questions asked in the literature and in practice is associated with the legal character of Bitcoin or, more generally, of cryptocurrencies¹²⁹. (Knnapas, 2016) (Lenz, 2014) (Regulation of Bitcoin in Selected Jurisdictions, 2014). That issue highly exceeds the framework of this study and should be examined in separate scientific research, not only from the point of view of private law, but also financial law, tax law, etc., so it is not going to be discussed extensively in this publication. However, an analysis will be presented of the legal relationship among the participants in the Bitcoin-creation process and its trading from the point of view of using the blockchain technology. The difficulty with describing these relationships and their legal character follows from the global character and simultaneous participation of multiple entities from practically every country in the world, and thus from different legal frameworks, as well as the technological character of those relationships and the anonymity of entities. Many debaters even claim that no codified laws function or apply to the generation

127 See N. Roth: An Architectural Assessment of Bitcoin, p. 531.

128 N. D. Bhasar, D Lee Kuo Chuen: Bitcoin Mining Technology, p. 47.

129 See D. Yermack: Is Bitcoin a Real Currency?, p. 31 et seq., A. Kristof: National Cryptocurrencies [in:] Handbook of Digital Currency, p. 67; K. Knnapas: From Bitcoin to Smart Contracts: Legal Revolution or E.volution from the Perspective of *de lege ferenda*? [in:] The Future of Law and eTechnologies, ed. T. Kerikmae, A. Rull, Cham, Heidelberg, New York, London, 2016, p. 111; Karl Fridrich Lenz, Japanese Bitcoin Law, publication of 2014 r, p. 8 et seq.; E. Ducas, A. Wilner, 2017, p. 538 et seq.

of bitcoins, replaced with the technological development of laws in cyberspace. That position is difficult to accept, but the discussion (Kerikmae and Rull, 2016) and potential international regulations for the digital economy, including digital tax, seem advisable.

Despite their technological character, the entities participating in the process of creating and trading in bitcoins are linked with numerous legal relationships, including contracts. This analysis will present only the ones related to or associated with the Bitcoin blockchain (due to the framework of this study).

The main legal relationships associated with the Bitcoin blockchain include: 1) the relationships between the Bitcoin blockchain creators and “miners”; 2) the relationship between the Bitcoin creators and the entities transferring bitcoins, 3) the relationships among the “miners” entering blocks in the Bitcoin blockchain, 4) the relationships between those transferring bitcoins and those placing “orders” for entries in the blockchain, 5) the internal relationships among miners within the given “digger” and 6) the relationships among the cryptocurrency exchanges and other participants.

License for Bitcoin software

The concept of Bitcoin and of using it for cryptographic work (digging), as well as trading in Bitcoin (transfers among entities) are possible thanks to the work of miners using stronger and stronger machines for calculating problems, accepting transactions and entering them in blocks, for which they obtain transaction (facultative) fees and participate in digging the next pool of bitcoins for correctly calculating the problem and adding a block. Anyone can become a miner by downloading the Bitcoin software and its whole blockchain, with all the blocks recorded to date. By doing so, in a way they join a distributed book by storing it. “Miners” are not the only ones joining the Bitcoin blockchain by installing the software and database of recorded blocks – the Bitcoin blockchain is also used by the Bitcoin authorities when they want to transfer it independently to another entity (the so-called wallet in the system is necessary for such a transfer). For an IT specialist, it “just” consists of downloading software and a database, similarly to a factual act. For a lawyer, it constitutes a contract, concluded online, available for all entities and on every territory, also (at least theoretically) outside of any territory (e.g., by downloading the software to computers on a space station in orbit).

Bitcoin is not only a technical solution that uses cryptography for securing “digital cash”, but, first and foremost, a concept for development of “digital cash” through a designed and launched ICT system without a central issuer (central authority) controlling the issue. In Bitcoin, neither the state nor public authorities decide on issuing a currency or its size. The principles of creating Bitcoin were developed by its authors (or author), creating a very complicated cryptographic algorithm, by specifying the amount of bitcoin in a precise manner and by specifying how often it would be “provided” to the market (thus, in fact, creating the first smart contract). The concept of Bitcoin was published under the pseudonym of Satoshi Nakamoto in a modest nine-page document entitled “Bitcoin: A Peer to peer Electronic Cash System”¹³⁰. The actual creator or creators of that concept have not been revealed to date. The idea behind the concept was not only to describe it theoretically (which had already happened earlier) but to actually create it, launch it and place it in the software network based on a very complicated algorithm used for generating Bitcoin, among others on the basis of the blockchain technology.

In legal terms, the author (or authors) of the software provided it anonymously based on an MIT license (open-source). Anyone can use it, modify it or disseminate it on other conditions without the source code¹³¹. What is only required is that the notes on copyrights and license are retained. The contents of the published declaration, regardless of the legal-copyright qualification as a license,¹³² excludes the possibility to consider the Bitcoin blockchain a work, the rights to which have been renounced.

The very contents of the license are quite concise:

The License (MIT)

	Copyright (c) 2009-2018 The Bitcoin Core developers
	Copyright (c) 2009-2018 Bitcoin Developers
	Permission is hereby granted, free of charge, to any person obtaining a copy

130 <https://bitcoin.org/bitcoin.pdf>.

131 The MIT license is one of the most liberal open-software licenses. It provides users with full rights to copy, use, modify and distribute (with or without payment) both the original or the modified program. The only requirement in the license is to provide information on the author.

132 Discussion of that issue exceeds the framework of this study.

	of this software and associated documentation files (the "Software"), to deal
	in the Software without restriction, including without limitation the rights
	to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
	copies of the Software, and to permit persons to whom the Software is
	furnished to do so, subject to the following conditions:
	The above copyright notice and this permission notice shall be included in
	all copies or substantial portions of the Software.
	THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
	IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
	FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
	AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
	LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
	OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
	THE SOFTWARE.

133.

It was not the first open-source license. Other examples include Linux, the source code of which is provided free of charge in such licenses as GPL (General Public License), LGPL (Lesser General Public License) or BSD (Berkeley Software Distribution License). However, the authors of the kernel of the Linux software are known, and the Linux Foundation has the right to use the name Linux and controls the use of the Linux name, and protects Linux users against patent violations as well as other legal threats¹³⁴ – it is a non-profit organization established with merger of two Linux organizations: Free Standards Group and Open Source Development Labs.

In the case of the Bitcoin software – not only is there no formal organization that would manage the licenses, but also the authors granting the

133 <https://github.com/bitcoin/bitcoin/blob/master/COPYING> of 6 November 2018.

134 <https://www.linuxfoundation.org/about/> of 6 November 2018.

license are unknown. It is unknown of which state they are citizens, from which state the software was published online, and its data immediately distributed online, making it impossible to locate it “physically” (to indicate the place from which it was published online), which makes it difficult to find from the point of view of international private law. Such activity by the software authors was fully intentional, as practical application of the “autonomy of the will” as the source of law¹³⁵, and the space of publication of the software and license is “cyberspace”, separate from any territory and justifying the so-called *lex electronica*¹³⁶. In practice, despite a number of statements that Bitcoin software substitutes “classic” law and “downloading the software” and starting to “mine for bitcoins” do not require any contracts, which might indicate it is a factual act, it is a classic license contract concluded between an identified, specific licensee and the licensor functioning under a nickname who is currently impossible to identify. However, this does not mean that it is not the case of an agreement between two entities. All in all, multiple contracts, including those common and performed immediately, are concluded anonymously or partially anonymously (when only one party is anonymous). This applies both to traditional contracts (e.g., shopping in a store in exchange for cash) and the digital economy (concluding a software license agreement). Usually, in the case of a software license, particularly a free one, the licensor is identified while the licensee remains anonymous. In the case of the Bitcoin software, the licensor is also anonymous, which does not happen frequently, but has been known to happen. A contract related to the Bitcoin blockchain is automatically performed by installing the software and all the previous blocks.

Bitcoin does not function in a legal vacuum¹³⁷ (Szostek and Swierczyński, *Wpływ nowych technologii na prawo prywatne międzynarodowe*, 2017). The fact that it is impossible to indicate the actual licensor, its registered office or place of granting the license, does not mean that laws do not apply.

135 See also chapter I.

136 More on the term *lex electronica* – P. Trudel: *La lex electronica in: Le droit saisi par la mondialisation*, ed. Ch. A. Morand, Brussels 2001 p. 221.

137 See also D. Szostek, M. Świerczyński: *Wpływ nowych technologii na prawo prywatne międzynarodowe*, [in] *Experientia docet. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Traple*, ed. P. Kostański, P. Podrecki, T. Targosz, Warsaw 2017 p. 1314 et seq.

The issue of new technologies and their impact on international private law was mentioned by P. Machnikowski¹³⁸ (Machnikowski, 2015), who stated that new technologies based on the Internet and computational clouds have unlimited, or even unspecified, territorial scope of application, and their operation results from engagement of entities and devices situated in different parts of the globe. This increases the significance of conflict-of-law principles and decreases the practical significance of domestic standards of obligations. He also stated that we should expect increased significance of intellectual-property laws at the cost of law of obligations and, to a higher degree, at the cost of property law¹³⁹. Bitcoin is a classic example.

For a contract concluded between a “miner” and the software author, it becomes necessary to look for the applicable law to determine what kind of law (real, territorial) applies to that contract.

The problem is that protection of intellectual-property rights is subject, as a rule, to the laws of the state, in the territory of which one is seeking that protection, both in terms of scope and means of protection – it is the so-called principle of territorialism¹⁴⁰. (Grzybczyk, 2015). The author indicates that the request for protection against violations of the copyright to online works¹⁴¹ requires indication of the state in which the violation occurred. However, it is uncertain whether it refers to the state in which the intellectual property was published online (which is impossible to determine in the case of the Bitcoin blockchain software) or to the state in which it is made available online¹⁴².

As a rule, the issues of the copyright status are subject to assessment based on *legi loci protectionis*, i.e., the principle of territorialism. That principle determines the subject of protection and creation, contents and expiry of copyrights. The subject literature indicates the problems of indicating the law applicable to the subject of copyrights, in particular the party originally entitled. The Bitcoin blockchain software, or actually its publication method, makes it even more difficult. “Two solutions are proposed:

138 P. Machnikowski: Prawo zobowiązań w 2025 roku. Nowe technologie, nowe wyzwania, [in] Współczesne problemy prawa zobowiązań, ed. A. Olejniczak, J. Haberko, A. Pyrzyńska, D. Sokołowska, Warsaw 2015, pp. 379-380.

139 P. Machnikowski: wo zobowiązań w 2025 roku, pp. 379-380.

140 K. Grzybczyk [in] System Prawa Prywatnego. Vol. 20c Prawo prywatne międzynarodowe, ed. M. Pazdan, Warsaw 2015, p. 7.

141 A separate issue that requires a more in-depth review is the issue of computer programs as works.

142 K. Grzybczyk [in]; Prawa Prywatnego. Vol. 20c Prawo prywatne międzynarodowe, ed. M. Pazdan, Warsaw 2015, p. 8.

the law applicable to indicating who is the author should be the law of the protecting country if we consider that the purpose of copyrights is to protect the author against abuse and to provide them with compensation for using its works. In such a case, the law applicable to indicating who is the author should be the same as the law that provides it with protection and compensation. Under another concept, the applicable law is the law of origin of the work, because it is the author who makes the decisions on developing the work, its shape and first publication. As technical capacity has made public availability global, the starting point for exercising a right should be one, clear and identical”¹⁴³.

Unfortunately, neither the author/authors of the Bitcoin blockchain software nor its/their country of origin are known. We do not know the country of first publication online. The conflict of law provisions and concepts applied until now do not apply to that case (currently). However, if the author/authors of Bitcoin blockchain are revealed, which is possible, at least theoretically, and practically not out of the question, the standard conflict of law principles and standards will be fully applicable. It should also be noted that it is more of a theoretical-legal issue, because, in practice, the issue of authorship of a work is not of primary importance, because “in most legal regulations related to copyrights, the status of the author is assigned to the actual creator who is also the entity originally entitled under property copyrights”¹⁴⁴.

To indicate the law applicable to contents of copyrights, the selected law is usually that of the state, for the territory of which protection is requested, and it should be law applicable to both the property rights and personal rights of the author. In this case, there is no problem with indicating that law, but in the case of the Bitcoin blockchain this means the possibility to indicate a number of laws, depending on the country, in the territory of which protection is requested which, it seems, has not been the intention of its author/authors.

We should also present the views of professor J. Barta and professor R. Markiewicz from twenty years ago:

“(…) the law applicable to seeking protection of copyrights is the law of the state in which the prohibited use of the work took place (*lex loci protectionis*). That law should determine the issues of the first entity

143 K. Grzybczyk [in]: Prawa Prywatnego. Vol. 20c Prawo prywatne międzynarodowe, ed. M. Pazdan, Warsaw 2015, p. 10.

144 K. Grzybczyk: [in] System, p. 11.

vested with copyrights, of meeting the premises of works, contents, scope and period of protection. From the point of view of international computer networks, this means application of the laws of all the countries in which the work is used by the end user (...). However, regardless of interpretation of the *lex loci protectionis* status, invoking it results in the need by the court of the given country to apply a whole “bundle” of foreign copyrights, which will cause serious difficulties in the cases of significant differences between the two systems¹⁴⁵ (Barta and Markiewicz, *Internet a Prawo*, 1998).

The difficulties described have forced the authors to seek a more lasting and universal criterion. That is why they suggested the possibility of taking into account the *lex loci originis* statute and the law of the country in which the operation of the given work started online, at the same time indicating a number of problems with applying it, such as the significant and frequent difficulty with determining that law in the case of works using international networks, but also the problem of differences between statutory laws in terms of basically all the aspects of copyrights which, in the case of *lex loci originis*, would force those participating in trading, as well as regular citizens, to respect the mandatory laws regarding the works or contents that they do not know. They also indicated the concept presented by C. Ginsburg, who stated that if a violation of copyrights takes place in several states, one should consider the possibility of accepting, as applicable law, the copyrights of the state in which defense is sought (*lex fori*) if the given country is the place where either a) the illegal use of the work started or b) the defendant has its place of residence, registered office, conducts business activity, or of which it is a citizen¹⁴⁶.

The above quick analysis indicates that, despite anonymity, lack of specification of the states in which the work is published online, etc., lawyers do not have to refer to the concepts of cyberspace or *lex electronica* to indicate the law applicable to the Bitcoin blockchain copyrights. Although so far there have been no court proceedings related to rights to the Bitcoin blockchain software, it is not impossible that they will appear in time, especially considering the value of bitcoins created and already existing amounts to many millions of dollars. So far, in the cases of disputes among those participating in the Bitcoin blockchain, there have appeared divisions among the participants and derivatives have been developed on the

145 J. Barta, R. Markiewicz, *Prawo zobowiązań w 2025 roku*, pp. 183-184.

146 J. Barta, R. Markiewicz: *Prawo zobowiązań w 2025 roku*, p. 186.

basis of the Bitcoin concept or its source code (e.g., Bitcoin Cash). This does not mean, however, that it is going to be like this forever. It is also possible that the actual authors of the Bitcoin blockchain will reveal themselves (although a lot indicates that it is rather improbable).

Development of various types of IT programs based on the Bitcoin source code or license is very intense nowadays. The subject literature indicates that as many as several new cryptocurrencies based on that license appear every day, not to mention other systems based on the distributed ledger concept. Two clear trends are visible: using the Bitcoin software source code to a higher or lesser degree (and thus using the license) and using it further, usually for commercial purposes (e.g., cryptocurrency exchanges); or using the concept of blockchains but with independent development of the source code and further software (without the need to use the Bitcoin software license). The phenomenon of fast development of open-source software is commonly known. An example is Linux, which was developed as a result of involvement of IT specialists being “enthusiasts”, who made the source code available without charge, a code which is still used today by such ICT systems as Android, the IT systems of the so-called supercomputers from TOP500, routers, cell phones and many other devices we use.

The blockchain technology introduced in Bitcoin (cryptocurrency) may be used, as an idea and a concept, independently of the Bitcoin software. There are no subject, territorial or legal restrictions (as a rule, an idea is not subject to copyright protection) for the possibility to prepare and implement software based on blockchain recording and cryptographic authorization, which can currently take up different forms and be based on various technologies. The term 'blockchain' is not limited to one technological method of recording data.

Other contracts within the Bitcoin blockchain

Within the Bitcoin blockchain, the software license is supplemented with a number of other contracts among the Bitcoin system users. The following relationships exist:

1. among “miners”
 - a) at entry in the blockchain,
 - b) within “joint digging”;
2. between holders of Bitcoin and the authors of its software,
3. between Bitcoin holders and recipients of transfers;

4. between Bitcoin holders and the entrepreneurs being the intermediaries in bitcoin-related activities.

The typical property of all these contracts is their global character as well as the digital environment in which they are concluded. What is also important is the ease of concluding them, the liberal attitude to their form, as well as a significant degree of anonymity (which has recently been changing to a high degree). An analysis of these contracts indicates different legal systems, as a result of which the judgments issued are not consistent. This is emphasized by, among others, the Draft Resolution of the European Parliament adopted on 16 May 2018 by the Committee on Industry, Research and Energy of the European Parliament suggesting (in the greater scope of DLT and only of the Bitcoin blockchain) development of a legal framework that would allow uniform seeking of claims at the Community level.¹⁴⁷

Relationships among “miners”

The basis of functioning of the Bitcoin blockchain system is the work of the “miners” who, in practice, verify the data recorded in the Bitcoin blockchain, make complicated cryptographic calculations, add entries to blocks, accept blocks, store the whole database on their devices, are the “nodes”, decide on changes in the algorithm (a decision on such a change requires the consent of a majority of “nodes”) and mine new bitcoins.

As a rule, anyone can become a miner. It can be a natural person or another legal entity. There are no territorial or technical restrictions in that regard. From the technical point of view, if someone wants to function as a “miner”, they just need to download and install the Bitcoin blockchain software, to download and archive the whole database of existing and recorded blocks, and to launch the software. From the legal point of view, it is not so obvious, though. Regardless of the legal system, for a contract to be effectively concluded, it is necessary to have legal capacity and the capacity for acts in law. Lack or limitation of legal capacity or capacity for acts in law may, depending on domestic laws, even result in invalidity of the legal transaction (in the case of a contract). This applies both to the license agreement related to the Bitcoin blockchain and to other contracts

147 http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/RE/2018/05-16/1144650PL.pdf of 11 July 2018.

concluded by a “miner”¹⁴⁸. To determine legal capacity or capacity for acts in law, it is necessary to find the criterion indicating the applicable law. The solutions are very diverse.

“The differences apply not only to criteria but also to how the scope of conflict-of-law standards are applied to natural persons. The criterion of citizenship is still frequently used as the main indicator of the personal rights of a natural person. However, it is currently competed with by the criterion of place of residence as well as the place of habitual residence of a natural person. In many legal systems, the same conflict-of-law standard covers both legal capacity and capacity for acts in law. However, in some legal systems these two notions are subject to different jurisdictions. Sometimes both standards use the same criterion. Other times, however, the criteria in both standards are different”¹⁴⁹¹⁵⁰ (Pazdan, 2014).

If a “miner” is not a natural person (which appears more and more frequently, among other reasons on account of the need to possess more and more stronger equipment for calculations), it is necessary to find the proper criterion for determining its legal subject status. That term covers both

148 Under German law, that issue is regulated by art. 104 and 105 BGB Geschäftsunfähig ist: 1.wer nicht das siebente Lebensjahr vollendet hat, 2.wer sich in einem die freie Willensbestimmung ausschließenden Zustand krankhafter Störung der Geistestätigkeit befindet, sofern nicht der Zustand seiner Natur nach ein vorübergehender ist. (art. 104) (Art.105 Die Willenserklärung eines Geschäftsunfähigen ist nichtig. Nichtig ist auch eine Willenserklärung, die im Zustand der Bewusstlosigkeit oder vorübergehender Störung der Geistestätigkeit abgegeben wird.

149 M. Pazdan [in] System Prawa Prywatnego, Vol. 20a. Prawo prywatne międzynarodowe, ed. M. Pazdan, Warsaw 2014, p. 557.

150 The states where the status of legal capacity is subject to *lex patriae* (of the country of citizenship) include, among others: Albania, Austria, Belgium, Bosnia and Herzegovina, Croatia, Bulgaria, France, Lichtenstein, Macedonia, Poland, Portugal, Ukraine, Hungary, Egypt, Qatar, South Korea and Turkey. It is subject to *lex domicilii* in, among others: Brazil, Estonia, Lithuania, Latvia, Paraguay, Peru and Venezuela. A hybrid system is used in, among others, Chile, the Dominican Republic and Columbia. In turn, the Czech Republic and China adopted the criterion of place of habitual residence. The USA and Great Britain lack the provisions regulating the jurisdiction of legal capacity. They usually accept the jurisdiction of *legis domicilii* (although domiciles are understood in a particular way). However, *legis domicilii* is replaced with *legis loci actus* with regard to capacity for acts in law. As for obligation agreements in the USA, what usually applies to assessment of capacity is either the law of the place where the agreement was concluded or another law applicable to the agreement.

legal personality and the legal capacity of the organizational entities that are not legal persons. There are many criteria¹⁵¹ indicating the applicable law, including: on the basis of the theory of registered office, a company is subject to the laws of the state, in which its registered office is situated; in the theory of incorporation, a company is subject to the laws of the state, under which it was established, etc.

Therefore, lawyers have the instruments to indicate the applicable law for the purposes of determining the status of legal capacity, capacity for acts in law, legal subject status, etc. The citizenship, place of residence, the center of vital interests, registered office and place of incorporation of each particular “miner” will be different, depending on whether they are natural or legal persons, and so will their criteria and applicable laws. A serious problem may appear in the foreseeable future with development of artificial intelligence that may be able to perform “acts in law”. That issue exceeds the framework of this study and requires an analysis not only in terms of blockchains but from a broader perspective.

In the Bitcoin blockchain, one may not determine all the entities accepting a block, or their subject status and whether they have the capacity to perform acts. In theory, this could affect the problem of determining the validity of an entry, making a transfer, etc. In practice, the number of “miners” participating in the process of developing a block is so high that, even if one or even many of them are considered not to be legal subjects, thus not being able to conclude a contract (for a license or including other obligations), the entry made by the remaining “miners” is still valid.

From a legal point of view, downloading software, launching it, downloading the whole blockchain database to one’s own device and, in particular, joining the blockchain system and to the remaining nodes, including by starting to “mine”¹⁵² or verify the data recorded, calculating the problems or accepting cryptographically the blocks must be considered a contract.

The authors and, currently, all the Bitcoin blockchain users (the majority of whom may change the principles of creating Bitcoin, including by introducing changes in the algorithm) have made the decision on the adhesive character of the contract. A new participant either agrees to follow the principles of functioning of the Bitcoin blockchain or is not allowed to

151 For example, in the USA, it is the criterion of establishment (depending on the state).

152 See the instruction video for how to mine Bitcoin <https://www.youtube.com/watch?v=NkH3ZKRyKy4> of 11 November 2018.

join the system. From a legal point of view, it either accepts the contract by adhesion or it will not be concluded with it. The typical property of a Bitcoin blockchain contract is its global, but also technological, character¹⁵³. It is a classic example of a smart contract. It is a multilateral contract consisting of cooperation in recording data in blockchain blocks and cryptographically securing that data, as well as recording and storing it on one's own device or devices, as well as making it available to other nodes. The issue of the payable character of the contract is problematic. Downloading the software and “mining” do not guarantee any remuneration. In the Bitcoin blockchain contract, there appears the random element of assigning 12.5 BTC to one of the “miners” (currently, that value decreases by half every four years) which, sometimes, is called a “reward” in the literature. It may only be assigned to the miners that have correctly calculated the result of the problem set by the algorithm, which is only possible as a result of a gigantic number of attempts to enter the correct number¹⁵⁴. The algorithm does not guarantee a “reward”; only the possibility to participate in drawing it.

The classic principles and criteria should be applied to determine the law applicable to the respective elements associated with concluding a contract, separately for each entity, resulting in a different applicable law in each case. However, there are no legal obstacles to indicating it.

However, indicating the law applicable to the whole Bitcoin blockchain contract would be a little difficult. There are no obstacles to indicating the applicable law in the contract (the acceptance thereof takes place by clicking when downloading the software). The admissibility of choice of law

153 The software may be downloaded from: <https://miner.nicehash.com> of 11 November 2018.

154 See M. Grzybowski, Sz. Bentyn: *Kryptowaluty*, 2018 (Cryptocurrencies) p. 35. The authors indicate that “the aim of each task is to provide the “evidence of work” consisting in calculation of the function of the SHA256 hash for the data included in the given block. Each block contains a reference to the previous block, a list of current transactions and the so-called nuance, i.e., a variable that is the basis of the problem. A difficulty occurs when the algorithm imposes the value of the first character that the solution is to contain. For a bitcoin “miner” to receive the reward, they have to calculate the hash function in the given block, starting from the given sequence of characters (...). By substituting any sequence of character at the end of a block, machines keep attempting to select the value of the nuance so as to find the result, the first character of which will be zero (...).” Which miner receives the BTC is, in a way, up to a sort of drawing of lots among the miners – which takes place, on average, every 10 minutes on a new dataset.

would be specified by the statute referring to the respective entities. Unfortunately, the Bitcoin blockchain contract lacks such a clause¹⁵⁵, which causes the need to look for other criteria. In this case, the behavior of the authors of the Bitcoin blockchain seems intentional in order to avoid the possibility of indicating one proper legal system. Nowadays, in the respective countries various concepts are functioning regarding the criteria indicating the law applicable to a contract in the case of lack of choice of law – these include, among others: the criterion of place where the legal act is performed, of the place of performing the obligation (often indicated as archaic), and there have been made proposals that the effects resulting in obligations should be assessed on the basis of *legis loci actus*, while the effects of that event should be on the basis of *legis loci solutionis* (or, actually, based on the law of the state in which the obligation should be performed). Despite criticism, the criterion of place of conclusion of the contract (*legis loci contractus*) or the criterion of place where the obligation is performed are also used. The theory of characteristic performance, developed and finally formulated by Adolf Schnitzer¹⁵⁶, is very popular in Europe, while the theory of the most suitable law, in British.¹⁵⁷ Some of those criteria (e.g., the place of concluding a contract or of performing legal acts) are impossible to apply because of the character and, in particular, the method of concluding a Bitcoin blockchain contract.

In the European Union, the law applicable to contractual obligations is specified by the Parliament of the European Parliament and Council (EC) No. 593/2008 of 17 June 2008 on the law applicable to contractual obligations¹⁵⁸, the so-called Rome I Regulation. Article 3 of that Regulation allows the freedom of choosing the law either upon conclusion of a contract or during its term. The fact that no law is chosen upon conclusion of a contract by participants in the Bitcoin blockchain system does not mean it may not be chosen at a later time (which might solve the problem of division of the status of the law applicable to a contract). In the lack of choosing the law, it results from provisions of the regulation, in this case art. 4. However, it would be difficult to use those provisions to indicate the law of one state. A contract among “miners” should be classified as an in-nomi-

155 11 November 2018.

156 See F. Snitzer, *L'autonomie des parties en droit interne et en droit international privé*, RDCDIP 1938, p. 243 et seq.

157 See also M. Pazdan [in:] *System Prawa Prywatnego*. Vol. 20b *Prawo prywatne międzynarodowe*, Warsaw 2015, pp. 46-48.

158 Official Journal of 4 July 2008r. L 177/6.

nate contract¹⁵⁹ (recording data, archiving it, making it available, cryptography, etc.), consisting of cooperation among partners, the performance of whom is characteristic to the same degree, and the democratized method of functioning results in the absence of an organizational entity that would allow someone to indicate unequivocally the law of one state with which its relationship is strongest. Also, neither its management board (because all the partners manage in a democratic and global manner) nor its registered office are possible to determine. The criterion of location of devices is not helpful either, because it may be random or multiple (in many states). It seems that the only criterion which may be useful and possible to apply is the place of habitual residence of a “miner” for the purpose of indicating the law of the state not only indicating the strongest relationship, but any relationship at all. Such a solution includes a number of significant disadvantages, mainly fragmentation of the statute, with all the consequences associated. It is far from optimum and raises a number of complications, but does not leave the lawyers helpless in their search for the law. The optimum solution for the Bitcoin blockchain partners would be to choose the law applicable to the contract, but in the absence of such a choice, applicable law should be sought in accordance with general principles of the law¹⁶⁰.

The provisions on provision of electronic services in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information-society services, in particular electronic commerce, in the internal market, do not seem to be a helpful source of the law applicable to the contract for entities operating in the EU¹⁶¹. It seems that directive, together with its domestic implementations, does not constitute a separate standard for conflicts of law, in particular the principle of state of origin resulting from art. 3 of the directive. The literature emphasizes that the character of that standard is not clear, particular in terms of principles of conflict of laws. Under art. 3, every Member States ensures that the information-society services provided by a service provider with its registered office in the given Member State be consistent with the domestic laws in effect therein, within the given field. However, the directive also includes the provision indicating that that directive does not establish additional principles regarding international private law and does not deal with court jurisdiction (art. 1 point 4), and also the recitals (point

159 The term 'agreement' in the Rome I Regulation has an autonomous character.

160 Problems require more in-depth scientific research

161 Official Journal of 17 July 2000, L 178/1.

23) indicate that the subject of the directive is not the introduction of additional principles of international private law applicable to conflicts of law or regulation of court jurisdiction. However, the provisions of the applicable law set by the provisions of international private law may not limit the freedom, set in that directive, of providing information-society services. That justification raises more questions than answers.

The legal character of art. 3 was performed by, among others,¹⁶² M. Świerczyński (Świerczyński, *Jurysdykcja krajowa a prawo właściwe*, 2004). He indicated that German and Austrian literature included as many as 4 positions:

“a) the concept of lack of interference of the principle of country of origin in international private law; b) acknowledgment of the principle of the country of origin as a conflict-of-law standard, excluding other conflict-of-law standards; c) adoption of the principle of country of origin solely as a recommendation in the scope of public law and; d) assumption that that principle refers directly to the given substantive law while bypassing conflict-of-law standards¹⁶³” (Fallenbock, 2001).

Under the first position, art. 3 sections 1 and 2, there should apply the law of the state where the registered office of the service provider is situated, as conflict-of-law regulation, but of general character which, in practice, is excluded by other conflict-of-law standards. In terms of substantive law, it applies to administrative or penal public law¹⁶⁴.

“Under that position, the court should start by determining the law applicable to the given case under the principles of international private law of member states, and if the given standard is less restrictive than the legal norm applicable to the registered office of the service provider, the court is obliged not to apply that standard.¹⁶⁵”

The second position assumes that the principle of state of origin is of conflict-of-law character. However, it is a conflict-of-law standard that consists

162 M. Świerczyński: *Jurysdykcja krajowa a prawo właściwe* [in:] *Prawo Internetu*, ed. P. Podrecki, Warsaw 2004 pp. 154-159 (cited as “*Jurysdykcja*, 2004”).

163 M. Świerczyński: *Jurysdykcja*, 2004, p. 155. See M. Fallenbock: *Internet und internationales Privatrecht*, Vienna 2001, pp. 195-204.

164 M. Świerczyński: *Jurysdykcja*, 2004, p. 156.

165 M. Świerczyński: *Jurysdykcja*, 2004, p. 156.

in referring to the law of the country of origin in the fields coordinated by the directive¹⁶⁶.

“In the third position, the country-of-origin principle is limited to public law and does not apply to private law and, in particular, does not violate the applicable principles of private law (...) The fourth one assumes that, as the law indicated on the grounds of the country-of-origin principle and the conflict-of-law standards of the law applicable to obligations may not be the same, it should be assumed that the country-of-origin principle does not refer to conflict-of-law principles, but replaces them. Therefore, it is assumed that the country-of-origin principle is tantamount to a substantive indication and not a conflict-related choice of law¹⁶⁷”.

Both M. Fallenbock¹⁶⁸ and M. Świerczyński¹⁶⁹ consider the second position correct with the reservation that art. 3 of the directive does not introduce a conflict-of-law standard excluding the application of other conflict-of-law standards, but only obliges the member states to establish such a conflict-of-law principle for the purpose of ensuring of application of the country-of-origin principle in the scope of private law. The significance of that order diminished as a result of the application of Rome I and Rome II regulations and of acceptance of the judgment issued by the European Union Court of Justice¹⁷⁰ in the Martinez case (combined cases No. C-154/15, C-307/15 and C-308/15).

The classification of activities of “miners” as “provision of electronic services” is not obvious. Under art. 2 point a of Directive 2000/31/EC, the definition of information-society service, included in directive 98/48/EC (art. 1 point 2), means the services normally provided at a distance and against remuneration, upon an individual request of the recipient. First, the implementations of the definition of “provision of electronic services” in the respective domestic systems, are not uniform. The problems are connected with the issue of miners’ remuneration, which is not guaranteed, some of which consists in creation by the system of a “reward” in the form of bitcoins. Assuming it is remuneration, it is not provided by other enti-

166 D. Dethloff: *Europaisches Kollisionrecht des unlauteren Wettbewerbsrecht*, Jus Privatum Bd. 54 2000rr, p. 57.

167 M. Świerczyński: *Jurysdykcja*, 2004, p. 157.

168 M. Fallenbock: *Internet und internationales Privatrecht*, pp. 203-204.

169 M. Świerczyński: *Jurysdykcja*, 2004, p. 157.

170 <http://curia.europa.eu/juris/document/document.jsf?docid=186483&doclang=PL> of 30 July 2018.

ties, but produced by the system. The literature indicates that remuneration does not have to be directly paid by service recipients. The provisions do not require the service to be paid for by the persons for whom it is provided¹⁷¹ (Polański, 2014). However, the problem refers to the phrase “individual request of the recipient”. When verifying data, each miner accepts it and enters it in blocks, making its data available through the node to all the other nodes, but also to the entities making up the cryptocurrency wallet. It happens automatically, practically without any knowledge of to whom and in what scope the blocks recorded in one’s own device are made available. It should also be noted that a miner” not only makes its data available and makes calculations, but also downloads it from others. From the point of view of providing information-society services, each miner would have to be simultaneously classified as a service provider and service recipient, which would still lead to fragmentation of the statute, indicating the law of the registered office of each “miner”. Taking into account the interpretation difficulties related to acknowledgment of the indicated provisions as conflict-of-law regulations, it seems that the provisions on electronic services may not constitute the sole basis for looking for applicable law.

Mining contracts

The growing need to make use of huge computing power for making calculations for a block within the Bitcoin blockchain makes it more and more difficult for a single person without professional equipment to “mine” a bitcoin. In the initial phase, the calculations required a “regular” computer, but with the growing difficulty of calculations (taking place, on average, every two weeks, or after calculation of 2016 blocks, to be exact¹⁷²), the computing power of a “regular” computer is becoming insufficient, and the calculations made – ineffective. For that reason, “mining contracts” aimed at “joint mining” are concluded more and more often. Such contracts are concluded not only for Bitcoin blockchains, but also for

171 More in P. Polański: *Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego*, Warsaw 2014, pp. 53-57.

172 So-called problem difficulty assessment. In theory, if the problem, in the last 2016 blocks, is too difficult to allow calculation in 10 minutes, that problem difficulty may be decreased. In practice, however, it is usually increased on account of the growing computing capacity.

other cryptocurrencies. Usually, such contracts are used by the entities planning to invest in mining cryptocurrencies but without the need to purchase equipment or operate software. They are usually concluded for a specified period of time and are of a diverse character. They are usually associated with the right to use the equipment of advanced “mining centers” and to use the computing power of the devices installed there, to which the service recipient connects using a computer solely for the purpose of communication with the “center” or for storing the cryptocurrency in the so-called wallet.

There are several types of mining contracts:

1. hosted mining – in which the user leases the user hosted by the provider. In such contracts, computing power is consolidated by large hosting providers who are able to control the network to some degree;
2. virtual hosted mining – in which the user creates a “private virtual” server for mining cryptocurrencies, on which they can install their own “mining” software;
3. leased hashing power – in a way, the user joins (invests in) the computing power of a data-center operator responsible for the equipment and software who, in exchange, receives some of the newly generated bitcoins. The disadvantage of that solution is lower profits, while the advantage – the lack of the need to operate equipment or software. In practice, that type of contract often turns out to be unprofitable.

The typical quality of the above contracts is professionalism of activities, where an entity that is professional, to a higher or lower degree, usually provides services to non-professionals. There is no problem with determining the location of registered residence of the service provider or of the characteristic performance. The general conflict of law principles are applied to the indication of applicable law.

A characteristic contract among “miners” is a “mining pool” contract, which consists of establishing a “group or groups of miners” who make joint use of their equipment and the computing power of their devices. Participation in such a group increases the probability of solving a problem for a block, and becomes less risky than acting on one’s own. The bitcoins obtained are distributed among the group participants pro rata to their contributions (computing power provided). A group is usually established by a group operator who collects its remuneration in the form of transaction fees for entering the data in a block faster. The amount and type of payment received is specified in the contract. Different operators use differ-

ent remuneration methods¹⁷³. These may include such systems as Proportional, PPS, SMPPS, RSMPPS, CPPSRB, PPLNS, DGM, PPLNSG or POT (Bhaskar and Kuo Chuen, *Bitcoin Mining Technology*, 2015). As a rule, the participation of a professional entity as a mining-pool operator allows the avoidance of the problems with determining applicable law.

Relationships among Bitcoin holders

There many ways of obtaining a bitcoin. Apart from “mining” it, one may obtain it in many different ways, e.g., by purchasing it directly from another holder, from so-called “cryptocurrency exchanges”, in which the purchase and sale prices are determined by the free market, obtaining it in the so-called “cryptocurrency exchange bureaus”, which act as intermediaries in purchases, offering advice as well as performing technical and IT activities for the purpose of obtaining a bitcoin, in Bitcoin ATMs as well as using other, traditional methods, such as donation, exchange, inheritance, etc.

Wallets

Bitcoin does not have a physical counterpart and constitutes, in full, records in the Bitcoin blockchain blocks. The holder only has a private key allowing it access to the bitcoins recorded in the Bitcoin blockchain (assigned to the key). The keys are stored in the so-called wallets which may take a number of forms. These include¹⁷⁴: a) software wallets – wallets in the form of computer applications – software downloaded within the blockchain system and installed on a PC. Like in the case of “mining” software, installation of the application requires acceptance of a license¹⁷⁵ (it is an MIT license¹⁷⁶). Software wallets may be full or light. A full software wallet constitutes the whole base of blockchain blocks installed on the PC

173 See also N.D. Bhaskar, D. Lee Kuo Chuen: *Bitcoin Mining Technology*, pp. 59-64.

174 Prepared on the basis of K. Piech: *Podstawy*, p. 38 and <http://bitcoin.pl/poradniki/portfele/382-jaki-portfel-bitcoin-wybrac> of 12 July 2018.

175 The issue of law applicable to a Bitcoin-wallet software license is similar to the issue of a “miner's” software license. In the case of other currencies, it is the license obtained from the entity issuing the given currency.

176 <https://opensource.org/licenses/mit-license.php> of 12 July 2018.

of the holder. The holder then becomes a regular node, its bitcoins as well as all the bitcoins of other holders are recorded on its medium. A full software wallet requires a lot of free disk space (at the moment this publication was written – ca. 225 GB) as well as time for downloading and installing it (the first synchronization may take even several days). For Bitcoin, the Bitcoin Core wallet is used (the official Bitcoin wallet), installed from the bitcoin.org website and which constitutes a full node of the Bitcoin network. It needs to be fully synchronized to operate properly. If it is not used for a considerable period of time, it will also require synchronization as well as downloading the Bitcoin blockchain blocks recorded since the last one. These blocks are downloaded from other system users. The next step is encrypting the wallet to prevent third-party access. Many addresses may be assigned to a wallet and used for accepting or transferring bitcoins for other holders. The address functions similarly to a bank-account number, with the reservation that many addresses may be assigned to one wallet. What is very important is ensuring the wallet is protected against third-party or malware attacks. There are several good practices: keeping a wallet on a virtual encrypted partition (hard drive or flash drive), or using a separate operating system (preferably Linux) installed on a separate partition or virtual machine; making regular copies¹⁷⁷ of the wallet (of the `wallet.dat` file) – deletion, destruction or loss of the wallet is tantamount to losing all the bitcoins collected therein, if you do not have a copy; b) a light software wallet is an application that also requires license permission, but in that case the blockchain and holder's bitcoins are not stored on a PC, but on the servers to which it is linked using an application. The light software wallet, so-called light Bitcoin blockchain wallet called Electrum¹⁷⁸, does not require the downloading of the whole blockchain; it is recorded on a remote server. There is no need to synchronize data, and a copy of the wallet is made remotely. Upon installation, it is important to write down or remember the so-called “seed” value which allows recovery of the wallet. The “seed” value may also take the form of a QR code that can be scanned using mobile devices to recover the wallet (the QR code printout or recording should be safely stored). One may install an official, offline version of Electrum (preferably on a separate computer not connected to the network or on an external memory disk). The online wallet is then used for sending

177 The good practices of storing cryptocurrencies are consistent with the principles of storing other data. See D. Szostek (ed.) *Bezpieczeństwo danych i IT w Kancelarii Prawnej*, Warsaw 2018, p. 3 et seq.

178 A wallet may be downloaded from <https://electrum.org/download.html>.

and the offline wallet for signing¹⁷⁹. Another classification of wallets is: c) online wallet – e.g., a light software wallet – with online access, characterized by a high degree of mobility, but with security lower than that of d) a hardware wallet, in the form of a USB key, very secure but not very mobile. It may be used with any computer with a USB slot. Finally, there are e) other physical wallets, characterized by a lack of online connection. Wallets are used for storing (private or public) keys, being combinations of digits and letters, so these keys may easily be recorded on physical media such as paper (a wallet is then a document containing the keys), as a combination of numbers and digits or as a QR code. Specialist software¹⁸⁰ has appeared that facilitates the transferring of private or public keys to (regular or properly secured) paper with the possibility of additional security mechanisms (holograms, stickers, etc.). In practice, it consists of printing a document (preferably using a so-called laser printer without a smart chip, that does not retain printout data in its memory) with a public or private key that may be secured (by submitting a suitable document) using specialist tape with a hologram (which allows verification of document integrity)¹⁸¹. The appearance of such a document resembles a traditional banknote, and should be protected and stored as such. If you lose it, you will lose your keys and access to Bitcoin. It also allows a third party to transfer a bitcoin from a wallet¹⁸².

The type of wallet-related contract depends on what wallet is used and how the software that allows it to be held it is obtained. Downloading software is associated with a license. It may be free (like in Bitcoin Core) or not. The legal issues of the Bitcoin Core software license are similar to those of miners' software. In turn, there are no legal problems with determining the applicable law in the case of obtaining a license from other, usually identified, entities. The contract (concluded through acceptance and clicking) usually includes exclusion of liability for potential loss of the Bitcoin on account of using the given software. This does not mean lack of liability if, for example, the software is defective or improperly secured. General principles of liability apply then. In some wallets, a problem may arise with identification of the entity operating solely in the network, so it

179 See <http://bitcoin.pl/poradniki/portfele/384-electrum-lekki-portfel-bitcoin> of 12 July 2018.

180 For example <https://bitcoinpaperwallet.com> of 12 November 2018.

181 See https://www.youtube.com/watch?time_continue=94&v=a47rrYBWjWQ of 12 July 2018.

182 Transfer of a bitcoin through a Paper Wallet is similar to transferring cash and guarantees full anonymity.

is recommended that the wallets of known, reputable entities, with physical registered offices, be used. Using the software of unknown entities operating online, for storing regular money instead of in banks, means using anonymous, unknown entities. Determination of applicable law should take into account the fact that a bitcoin holder may be a natural person, as a result of which, in some cases, there may apply consumer-related clauses, such as art. 6 of the Rome I Regulation. However, it requires each time examination of the premises resulting from conflict-of-law provisions.

Transfers of bitcoins or other cryptocurrencies and blockchain records

The issue of legal character of Bitcoin or other cryptocurrencies, and thus of the transactions of transferring a cryptocurrency to another entity, requires separate, extensive scientific research, including comparative legal research and tax research, which exceeds the framework of this study. This point will only describe the civilist principles of bitcoin transfers but from the point of view of the subject of this monograph, i.e., blockchain technology.

A bitcoin may be obtained in different ways. By own activity, i.e., its “mining” using mining software, of random character, but also on the basis of contracts or other legal events.

As for the contracts being the basis for bitcoin transfers, we should each time look for the law applicable to the given contract, mainly in order to determine its character, and thus the admissibility and legal grounds for the transfer taking place as a result of performance of the contract. It becomes necessary to verify whether a legal act is of causal or abstract character. For the acts in law that bring benefits, in particular in most states of the European legal system, when activity validity depends on the correct *causae* (causal acts), it is necessary to verify the existence and validity of the *causae* being the basis for the benefit. However, there is no need for such verification for abstract legal acts. However, it should be remembered that most legal systems allow the abstract structure of legal acts solely in exceptional cases specified by legal provisions. In particular, the practical significance of the classification into causal and abstract acts is visible in the cases when the benefit is generated through a separate legal act. That is because in such a case the point is to determine whether its validity depends on another legal basis. In contracts with double effects, the considerations regarding *causae* are not so important, because, in practice, the significance and validity of the contract are examined through analysis of that legal act

and only to a lesser degree, of the *causae*¹⁸³. Basically speaking, there are three types of *causae*:

- a) *causa obligandi vel acquirendi* (the benefit acquires legal basis as a result of acquisition of a right or another benefit by the person performing the legal act);
- b) *causa solvendi* (the legal basis is release from an existing obligation which encumbered the person performing the act) and
- c) *causa donandi* – the benefit is provided free of charge.

An entity to whom a transfer has been made without legal basis or without the correct *causa* in causal legal acts, in civilist terms, may be treated as unjustly enriched and thus, may become obliged to return it in kind or, if it is impossible, to return the value of the benefits obtained in accordance with the provisions applicable to unjust enrichment. Claims for unjust enrichment in *common law* regulations are usually associated with the so-called “restitution law”.

“The basis for the general principle of lack of enrichment is in the American doctrine, in § 1 Restatement of the Law Regulation, Quasi contracts and Constructive Trust, published in 1937 by the American Law Institute, under which the person that has become unjustly enriched at the cost of another person, is obliged to return it”¹⁸⁴ (Mostowik, 2006).

In the countries of the European Union, the search for the law applicable to unjust enrichment is subject to Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations¹⁸⁵, referred to as Rome II.

The authors of the regulation wanted to regulate the issue of law applicable to assessment of non-contractual obligations regardless of the source thereof, with the reservation of a list of explicit exceptions. Under art. 10 of the regulation, if a non-contractual obligation on account of unjust enrichment, including of an undue benefit, refers to a relationship between the parties, such as the relationship resulting from a contract or from a prohibited act which is closely related to unjust enrichment, it is subject to the law applicable to that relationship. If applicable law may not be deter-

183 See Z. Radawński: *Prawo cywilne- część ogólna*, Warsaw 1993, p. 149.

184 P. Mostowik: *Bezpodstawne wzbogacenie jako źródło zobowiązania uwagi prawnoporównawcze*, *Problemy Współczesnego Prawa Międzynarodowego Europejskiego i Porównawczego*, No. 4/2006r. p. 20.

185 Official Journal of 31 July 2007 L199/40.

mined on the basis of the above principle, and the place of habitual residence of the parties, upon occurrence of the event being the source of unjust enrichment, is in the same state, the law of that state will apply. If applicable law may not be determined under section 1 or 2, the applicable law is the law of the state in which the unjust enrichment occurred (the location of the effect of the asset transfer is decisive). In turn, if it follows clearly from all the circumstances of the case that a non-contractual obligation on account of unjust enrichment is much more closely related to a state other than the state indicated in section 1-3, the law of that other state will apply. The conflict-of-law principle specified in art. 10 is of cascading character, which means that the subsequent principles may apply only in the lack of application of the previous ones.

“The issue of fundamental importance is setting the scope of the conflict-of-law standard based on art. 10 of the Rome II Regulation. That scope covers all the non-contractual obligations on account of unjust enrichment, not excluding undue benefits. Although the lawmaker used the terms of fixed meaning in domestic legal orders of the respective member states, it seems obvious that that understanding should not be transferred to the area of international private law. Just like in all the other cases, these terms should be interpreted based on the assumptions of autonomous classification¹⁸⁶” (Świerczyński and Żarnowiec, 2015).

An entry of a transfer of bitcoins or other cryptocurrencies in a blockchain does not validate a faulty legal act. Therefore, in civilist terms, in the case of, for example, theft of cryptocurrency or, for example, wrong entry of a wallet address and transfer of a cryptocurrency to the entity other than resulting from a contract, there exist the legal tools that allow return of the cryptocurrency that had been transferred by mistake or in violation of the law. Another issue is enforcement of such an entitlement. It is worth noting that even the legal presumption of § 1913 point 3) of title 12 of the Vermont Statutes (regulating the legal presumption of an entry in a blockchain) does not constitute a premise convalidating an erroneous transfer of a cryptocurrency recorded in a blockchain.

186 M. Świerczyński, E. Żarnowiec, *System Prawa Prywatnego*. Vol. 20B *Prawo prywatne międzynarodowe*, ed. M. Pazdan, Warsaw 2015, p. 840.

Cryptocurrency “exchanges” and buyers

A bitcoin or another cryptocurrency may be obtained by purchasing from another person, being a natural person, legal person or another entity with legal capacity. Cryptocurrencies are often traded using software that joins sellers with buyers, but more and more often professional websites (managed by actual entities) are used, so-called “exchanges”¹⁸⁷ that assist in selling and buying cryptocurrencies in exchange for a commission paid either in cryptocurrencies or traditional currencies. The global character of cryptocurrencies and the possibility to conclude an online contract make it possible to conclude a contract with any exchange in the world¹⁸⁸. The buyer should exercise special caution due to the vast number and localization of exchanges, also in terms of legal regulations. In recent years, many “cryptocurrency exchanges” have been attacked, “robbed” or gone bankrupt. One of the most infamous ones was the “theft” of 700,000 BTC of clients and 100,000 own BTC of the value of over half a billion dollars from the MT.Gox exchange in Tokyo. A similar “theft” took place in 2018 from the Coincheck exchange (losses of ca. 530 million dollars). Other “robbed” exchanges include Bitomat, MyBitcon, Bitcon7, Bitcoinica, Bitcoin-Central BTC-e and others.

Such currencies function (in terms of functionality and not law) similarly to security exchanges, where you may open your “accounts”, credit them with actual funds, e.g., using a standard bank transfer in zlotys, dollars or euros, through deposits in post offices, etc., and obtain cryptocurrencies in exchange. These exchanges allow you to store and trade in cryptocurrencies. On account of the attacks on “exchanges”, IT-security specialists warn against storing cryptocurrencies in them. The best idea is to store them in one’s own wallet.

The need to regulate the functioning of that type of institutions is becoming more and more urgent, not only for protection of cryptocurrency users (holders) but also of the institutions trading, all in all, in hundreds of millions of dollars. That issue is emphasized by, among others, the Euro-

187 The literature also includes the broader term “administrator”. See R. B. Levin, A. A. O’Brien, M. Zuberi : Real Regulation of virtual Currencies, p. 338 et seq.

188 An example of such an exchange is <https://coinmarketcap.com> or the Katowice BitBay, considered to be the largest Polish exchange in the CoinMarketCap ranking.

pean Commission, the European Central Bank¹⁸⁹, or financial-supervision authorities of multiple countries. The need for regulation is more and more often mentioned by exchanges themselves, invoking lack of legal protection of their activities. It seems that the initial period, a little chaotic and pioneering, is slowly turning into a relatively stabilized market of cryptocurrency trading. It should be noted that, when this publication was being prepared, the capitalization of the 100 largest cryptocurrencies was estimated at over USD 250 billion (13 July 2018).

One such regulation is the legal deed issued by the New York State Department of Financial Services New York Codes, Rules and Regulations Title 23 Department of Financial Services Chapter I, Regulations of the Superintendent of Financial Services Part 200, Virtual Currencies, also referred to as Bitlicense. Its section 200.3 indicates that it is prohibited to become involved in virtual-currency business activity without a license from the superintendent. The subsequent provisions specify the premises for obtaining a license, but also the rules of conducting licensed activity. Virtual, currency-related business activity includes:

- a) receiving a virtual currency for the purpose of transferring it further;
- b) securing, storing, holding, supervising or controlling a virtual currency on behalf of other persons;
- c) purchasing and selling of a virtual currency for a client;
- d) providing the services of converting or exchanging a virtual currency or a fiat currency; converting or exchanging a virtual currency into or for another currency;
- e) controlling, administering or issuing a virtual currency. The licensee is obliged to introduce a program of preventing money laundering which covers risk assessment, maintenance of documentation, and reporting of suspicious transactions and clients.

Also, an entrepreneur is obliged to block the transactions that violate the law (New York State Department of Financial Services, 2014a). For the purpose of protecting clients' assets, the licensee is obliged to maintain a bond account and trust account in USD in favor of its clients and to hold the virtual currency of the same type and amount, which is due to the clients that have allowed their virtual currency to be stored by the licensee. Also,

189 See the Legal Working Paper Series. Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks (October 2017), p. 2 et seq.; Virtual currency schemes – a further analysis (February 2015) p. 7 et seq. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>.

the licensee is obliged to inform its clients in writing of the significant risks related to virtual currencies in English and other languages dominant in the initial stage of relationship with the client and before conclusion of the first transaction. Additionally, there are capital requirements for those activities, including reporting. A complaint-processing policy is also required, and the licensee must state that the potential complainant may also submit a complaint with the New York State Department of Financial Services. Taking into account the fact that virtual currencies are electronically processed, in order to meet the security requirements, a qualified employee has to be designated to hold the position of security specialist, responsible for: the licensee's cybernetic security program, cybernetic-threat identification, electronic-system protection, unauthorized-access detection, as well as data recover after events related to cybernetic security¹⁹⁰ (Pak Nian and LEE Kuo Chuen, 2015).

"Cryptocurrency-exchange" regulations were also introduced¹⁹¹ in other states, such as Singapore¹⁹² (Lim, 2015), Japan, Switzerland and Belarus, where Decree No. 8 of the President of Belarus introduced the regulation regarding development of the digital economy¹⁹³. Under art. 2.3, cryptographic-platform operators and "cryptocurrency-exchange" operators are obliged to ensure availability on accounts in the banks of the Republic of Belarus of monetary means in the amount of not less than 1 million Belarusian rubles for a cryptographic-platform operator, and not less than 200,000 Belarusian rubles for a "cryptocurrency-exchange" operator. A cryptographic-platform operator is entitled: to open accounts in banks, non-bank credit-and-finance organizations in the Republic of Belarus and abroad for making settlements on trading and operations being carried out by them; to receive remuneration for services being rendered, including in tokens, to establish its amount and the order of collection from trading participants (customers); to perform (organize) transactions with residents and non-residents of the Republic of Belarus, aimed at placement of tokens, including abroad, acquisition and/or alienation of tokens for Belarusian rubles, foreign currency, electronic money, exchange of tokens for oth-

190 L. Pak Nian; D. Lee Kuo Chuen, A Light Touch of Regulation for Virtual Currencies [in:] Handbook of Digital Currency, ed. D. Lee Kuo Chuen, 2015 pp. 321-322.

191 E.g. California AB-1326 Bill, Digital Currency, status https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB1326.

192 J. W Lim: A Facilitative Model for Cryptocurrency Regulation in Singapore [in:] Handbook of Digital Currency, ed. D. Lee Kuo Chuen, 2015.

193 <http://law.by/document/?guid=3871&p0=Pd1700008e>.

er tokens in the interests of customers or in own interests; to perform (organize) other transactions (operations) with tokens, with the exception of operations on exchange of tokens for civil-right objects other than Belarusian rubles, foreign currency and electronic money.

Currently, the most interesting and one of the latest legal regulations related to virtual finance is the Maltese *Virtual Financial Assets (VFA) Act*¹⁹⁴ of 5 July 2018. In combination with two others (*Innovative Technology Arrangements and Services Act*¹⁹⁵ and *Malta Digital Innovation Authority Act*¹⁹⁶), that act regulates the manner of issuing tokens, state-authority supervision and protection of participants in token trading. However, as there are many types of tokens, a token may be considered not only a security or a financial instrument, but also a cryptocurrency or identification item.

One of the new terms introduced in the above-mentioned acts, of significant application to blockchain technology, is “*virtual financial asset*” (VFA), being any form of digital records used as a digital means of exchange, a settlement unit or value-storage unit, that does not constitute electronic money, a financial instrument or a virtual token. However, before such assets are allowed in the Maltese market, every VFA issuer must present the so-called “*Whitepaper*”, which constitutes documentation similar to a prospectus, containing information on the issuer, DLT technology and the product. In order to provide the necessary degree of security for participants in trading, there was introduced the requirement to submit a license application to the competent state authority (*Malta Financial Services Authority*) only through a proper, registered entity, called a VFA agent. Such an entity is required to demonstrate that the applicant is a person fit for providing the given VFA services and that it is going to meet the requirements of Maltese law.

However, it is not the only public-administration authority that participates in the whole license process. That is because a new authority was established – *Malta Digital Innovation Authority* (MDIA) – that supervises digital innovations. The basic task of that authority is to control the source codes of smart contracts, thus affecting the decision on granting a license.

194 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&cl=1>, access on 8 November 2018.

195 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&cl=1>, access on 8 November 2018.

196 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&cl=1>, access on 8 November 2018.

A similar source-code examination also applies to the DAO that want to function legally in the territory of Malta.

The above-mentioned license is an element necessary for conducting activities related to blockchains, as without the license such activities would be illegal.

The legal regulations associated with “cryptocurrency exchanges” and their activity are becoming more and more important due not only to the value of capital they trade in but also to user protection¹⁹⁷. Court decisions also indicate the need for proper regulations. An example is the decision from 2016 in the case of *Florida v Espinoza*,¹⁹⁸ which indicates a lack of regulations covering the specific character of Bitcoin and the need to adapt the statutory regulations of the state of Florida in the scope of cash services, to new technologies¹⁹⁹ (Patrick and Bana, 2017).

In particular, it is important to standardize the principles of functioning of “cryptocurrency exchanges” and to control them at least at the level of the community. Currently, global regulation, which would be optimum when taking into account the global character of activities of “exchanges”, seems impossible to introduce. It should be noted that criminals use that fact by “stealing” cryptocurrencies often from legal exchanges operating under the law, by quickly transferring them to the countries that do not regulate trade in cryptocurrencies, often exchanging them for other cryptocurrencies and, finally, for fiat currencies, for example using Bitcoin ATMs²⁰⁰. The legally operating companies are really interested in legislation, which is particularly visible in the Maltese market.

As regards the law applicable to the contracts between a cryptocurrency holder and “stock exchange”, there apply the general conflict-of-law provisions indicating the law applicable to the contract.

Blockchains or DLT and electronic money

The concept of Bitcoin and other cryptocurrencies appeared for the purpose of developing “money” or, actually, a whole currency system, func-

197 An example might be a Bitcoin casino online <http://www.bitbet.com> of 13 July 2018.

198 *Florida v Espinoza*, Case No FL14-2923 (Fla 11th Cir Ct) (22 July 2016).

199 G. Patric, A. Bana: Report Rule of Law Versus Role of Code: A Blockchain-Driven Legal Word, International Bar Association; November 2017 p. 16.

200 Over 1000 Bitcoin ATMs were functioning in the USA in 2017.

tioning in business transactions with the possibility of payment without banks or financial institutions (and their “power”), that would be self-regulating, based on democratic processes of making decisions on the currency and on the technologies applied (by a majority of users), functioning in digital space (cyberspace) on equal terms for all the users, based on the computing power of computers, alternatively to domestic and international regulations and legal orders, and the new money was to be “transparent”, fair and independent. Modern societies, particularly those of young and very young people, for whom the issues of borders, language or mobility are no longer problematic, who work and move globally – unlike the older generations – have a different attitude to state institutions or international organizations, the objective of which, for many years, has been to maintain the social order within the legal regulations developed and imposed. Their understanding of money and functions thereof is also different. Development of cryptocurrencies and of the currently utopian concepts of electronic money constituted, as indicated at the beginning of this chapter, a response to the archaic character of contemporary banks and payment methods without taking into account state-of-the-art technologies or the need to provide cheap and fast payments not so much in domestic relations (because these are usually available), but rather in international, including intercontinental, relations. It is especially associated with the development of the digital economy, in particular eCommerce, but also payments for digital content, online services and increased mobility of young society.

So far, during Bitcoin’s ten-year history, hundreds of new cryptocurrencies have not achieved the assumed objective – functioning without legal frameworks. The fall of “exchanges”, loss of cryptocurrencies, regular frauds, etc., have forced the cryptocurrency enthusiasts to change their views.

“It is an irony that their problems could be solved through regulation and integration with the financial-currency system, or even adoption of the existing business models of the payment and commercial-banking sector to which cryptocurrencies were supposed to oppose. New payment technologies will reach their full potential only after introduction of proper regulations²⁰¹” (Papadopoulos, 2015).

201 G. Papadopoulos: Blockchain and Digital Payments: An Institutionalist Analysis of Cryptocurrencies, [in:] Handbook of Digital Currency, 2015, p. 172.

It should be emphasized that cryptocurrencies and the institutions behind them have, in a sense, developed a trading market that is parallel, not so much alternative, because upon “entry” and exit it still requires traditional fiduciary money, currently estimated at over USD 250 billion (based on TOP100 cryptocurrencies), which may be impressive, but only constitutes a fraction of the global turnover. However, they are noticeable and should not be ignored. A lot, including pilot studies ordered by financial institutions and banks, indicates that blockchains and some other solutions related to cryptocurrencies will be used by financial institutions in the foreseeable future.

Examples include projects for developing electronic money²⁰² based on DLT and private blockchains. Electronic money was introduced in the Electronic legal system almost ten years ago in 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. It is legally regulated at the level of the European Community, in domestic implementations, and applies across the whole European Union. So far there has been not much interest in electronic money in European business trading, and it was mainly related to the so-called electronic money on a card. Development of cryptocurrencies and increased interest in them, as well as the distributed-ledger technology (DLT), including blockchains, indicate an increased interest in electronic money among Europeans, but also changing needs: money on a card is more and more often replaced with the so-called server electronic money or money on other electronic media, e.g., a cell phone. The whole trend, as well as the needs of citizens and entrepreneurs, was noticed by the EU, which introduced in 2015 Directive (EU) 2015/2366 of the European Parliament and of the Council 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 (so-called PSD2),²⁰³ which had been implemented by member

202 The literature also uses the term: “virtual currency” which might be defined as digital representation of value, not issued by a central bank, credit institution or electronic money institution which, in certain circumstances, may be used as an alternative to money. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencieschemesen.pdf> of 16 July 2018.

203 More on the PSD2 regulation: P. Rohan: PSD2 in Plain English: Volume 1 (Payment Landscape for Non-Specialists), Rohan Consulting Services Limited Dublin 2016, p. 4 et seq.

states in their legal systems until 2018. Therefore, it is new legislation that is significant for development of the electronic-payment market, including payments using electronic money.

The definition of electronic money is included in point 2 of Article 2 of directive 2009/110/EC and means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic-money issuer; On account of repealing directive 2007/64/EC, a “payment transaction” should be understood as a transaction specified in directive PSD2, in which two terms are included: “payment transaction”, meaning an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee; and “remote payment transaction”, meaning a payment transaction initiated via the Internet or a device that may be used for long-distance communication.

Under the recitals of Directive 2009/110/EC, the definition of electronic money should cover electronic money whether it is held on a payment device in the electronic-money holder’s possession or stored remotely at a server and managed by the electronic-money holder through a specific account for electronic money. That definition should be wide enough to avoid hampering technological innovation and to cover not only all the electronic-money products available today in the market but also those products which could be developed in the future.

This study is not aimed at a comprehensive analysis of electronic money or PSD2, but the issue of application of DLT and blockchains for creating it, as well as for making remote-payment transactions under PSD2, but it should be noted that the new legal regulation, implemented through complete harmonization, comprehensively regulates the issues of payment using electronic money, while being fully neutral in technological terms. There were specified the principles of exchanging a fiduciary currency for electronic money, the obligation to repurchase it, the principles of conversion (e.g., exchanging electronic money in EUR for electronic money in PLN), and a number of information obligations, the vast majority of which has to be provided on a durable medium (one of the solutions for durable media is the application of blockchain technology, as indicated below).

Under the new provisions, electronic money may be stored using software wallets (based on cryptocurrency terminology), i.e., using a wallet in

the form of an application, either in full or light form, or, based on another classification, in an online or hardware wallet, or even in other physical wallets, just like cryptocurrencies. The transactions using electronic money may be performed anonymously, but with the possibility of identification. Also, there are no obstacles to making further payments using the obtained electronic money entered in a blockchain (like a cryptocurrency). The principal difference between cryptocurrencies and electronic money consists of how they are created. In the former case, creation may take place using a public blockchain, but also a private blockchain (depending on the type of cryptocurrency), and in the latter – usually using a private blockchain, for which a third party, e.g., electronic-money issuer, is responsible. In the former case, it is difficult to specify the applicable law, while in the latter – the legal regulations are clear. In the scope of control over the entities that issue electronic money, the concept of Directive PSD2 is similar to the New York State Department of Financial Services New York Codes, Rules And Regulations Act.

It seems that the direction indicated by the EU in directive PSD2 is correct and consistent with the current needs and challenges associated with, among others, DLT. It allows the making of direct peer-to-peer payments without banks, using blockchains or DLT in a fast and low-cost manner, thus attracting cryptocurrencies. Blockchain technology may support the development of electronic money.

Chapter IV. Durable media with blockchain technology

Introduction

Most reports on the application of blockchain technology indicate the fields of finance and banking as some of the first and greatest beneficiaries of that solution. In practice, the financial sector was one of the first ones to undertake activities to use that technology, and was the first one with successful implementations in that scope.

The financial sector is not the only one interested in the technical aspect of “durable media”. Over the last four years, that term has substantially evolved, from a conservative, traditional (paper) perspective to a very modern one. It is not only the banking sector, or, more broadly, the finance sector, but also the eCommerce, telecommunications sectors, the sector of services not only of the digital, but also hybrid, economy (electronic acts and “traditional” goods), that are interested in its application, in particular in a modern “paperless” form.

Term of durable medium

The term, including the legal definition, of a durable medium, has been introduced in EU law and so, in the respective domestic legal systems, relatively recently. They are included in many pieces of legislation, often different ones.

As for Community regulations, the term or reference to it are included in, among others: Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC (OJ L 271, 9.10.2002, p. 16); Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation (OJ L No. 9, 15.01.2003, p. 3); Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (OJ L No. 133, 22.05.2008, p. 66); 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 (OJ L No. 304, 22.11.2011, p. 64); and Commission Implementing Regulation (EU) No 1203/2012 of 14 December 2012 on the separate sale of regulated retail roaming services (OJ L No. 347, 15.12.2012, p. 1).

In Community regulations, a durable medium should be understood in the following manner:

1. as defined in letter f of article 2 of Directive 2002/65/EC of the European Parliament and Council of 23 September 2002 – “(f) "durable medium" means any instrument which enables the consumer to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;
2. as defined in point 12 of art. 2 of Directive 2002/92/EC of the European Parliament and Council of 9 December 2002 – durable medium "means any instrument which enables the customer to store information addressed personally to him in a way accessible for future reference for a period of time adequate to the purposes of the information and which allows the unchanged reproduction of the information stored;
3. as defined in letter m of art. 3 of Directive 2008/48/EC of the European Parliament and Council of 23 April 2008 – durable medium “means any instrument which enables the consumer to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;”
4. as defined in art. 2 of Directive 2011/83/EU of the European Parliament and Council of 25 October 2011 – durable medium means any instrument which enables the consumer or the trader to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;
5. as defined in point 35 of article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council 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 – durable medium means any instrument which enables the payment service user to store information addressed personally to that payment service user in a way accessible for future reference for a period of time adequate to the purposes of the in-

formation and which allows the unchanged reproduction of the information stored.

The issue of s durable medium was also addressed in the judgments issued by the EU Court of Justice. In judgment C-49/11 (of 5 July 2012)²⁰⁴ the Court found that for the given medium to be considered durable, it is necessary to prove that a transmission of information with the use of that medium guarantees a lack of the possibility to amend the contents of the document delivered on such a medium, and guarantees availability in a suitable period, allowing consumers to recover the document contents in an unchanged form.

According to the Court, a website does not constitute an example of a durable medium, as defined in section 1 of article 5 of directive 97/7/EC, because the information included on a website is available to consumers solely by means of a link provided by the seller. The Court invoked the legal view presented in a judgment issued by the European Free Trade Association (EFTA) Court of 27 January 2010,²⁰⁵ that stated that a website may be considered a durable medium if it enables the customer to store information in an unchanged form in a way accessible for future reference for a period of time adequate to the purposes of the information. When issuing the judgment, the EFTA Court invoked, among others, the guidelines presented in a report by a European Securities Markets Expert Group (ESME)²⁰⁶.

In turn, in a recent judgment C-375/15 (of 25 January 2017), the Court of Justice of the EU considered that a Bank website (including the electronic mail within it), could be considered a durable medium, as it

“allows the payment-service user to store information addressed personally to that payment user in a way accessible for future reference for a period of time adequate to the purposes of the information and allows the unchanged reproduction of the information stored. Furthermore, for a website to be regarded as being a ‘durable medium’ within the meaning of that provision, any possibility that the payment-service provider or another professional to whom

204 CJEU judgement of 05.07.2012 in case C-49/11 *Content Services Ltd against Bundesarbeitskammer* (EU:C:2012:419, point 46).

205 Judgment of the European Free Trade Association (EFTA) of 27.01.2010 in case E-4/09 *Inconsult Anstalt ca. Finanzmarktaufsicht* (Official Journal of the EU C No. 305 of 11.11.2010, p. 16).

206 ESME’s report on durable medium – Distance Marketing Directive and Markets in Financial Instruments directive; http://ec.europa.eu/finance/securities/docs/esme/durable_medium_en.pdf [access: 11.11.2018].

the management of that site has been entrusted could change the content unilaterally must be excluded”.

The CJEU invoked the difference between the terms of “providing” and “making available” by the Bank website. It was indicated that

“the information concerned which is transmitted by the payment-service provider to the user of those services by means of an online banking website may be considered to have been provided within the meaning of Article 41(1) of Directive 2007/64, if such a transmission is accompanied by active behaviour of the provider aimed at drawing the user’s attention to the existence and availability of that information on that site”²⁰⁷.

The above judgments questioned the previous practices of banks (judgment C-375/15) but also of other entities (judgment (C-49/11) obliged to provide documents containing declarations of intent or the information, required by the law, consisting of publication of documents on the website of the entity obliged to provide them, without the possibility to “download” them so as to have permanent access to their unchanged contents. In other words, for the given IT tool to be considered a durable medium, the client must have free access to the information sent to that medium, including to documents, and their recording and storage on that durable

207 Justification of the judgment: *Articles 41(1) and 44(1) of Directive 2007/64/EC on payment services in the internal market, read in conjunction with Article 4(25) of that directive, must be interpreted as meaning that changes to the information and conditions, provided for under Article 42 of that directive, and changes to the framework contract as well, which are transmitted by the payment-service provider to the user of those services through the electronic mailbox of an online banking website, may not be considered to have been provided on a durable medium within the meaning of those provisions, unless these two conditions are met:*

– that that website allows the user to store information addressed to him personally in such a way that he may access it and reproduce it unchanged for an adequate period, without any unilateral modification of its content by that service provider or by another professional being possible; and

– if the payment-service user is obliged to consult that internet website in order to become aware of that information, the transmission of that information is accompanied by active behaviour on the part of the provider aimed at drawing the user’s attention to the existence and availability of that information on that website.

In the event of the payment-service user being obliged to consult such a website in order to become aware of the relevant information, that information is merely made available to that user within the meaning of the first sentence of Article 36(1) of Directive 2007/64, as amended by Directive 2009/111, when the transmission of that information is not accompanied by such active behaviour on the part of the payment-service provider.

medium must allow them to be recovered in an unchanged form for a suitable period of time.

Irrespective of whether the term “durable medium” refers to the banking sector and the regulations associated therewith, or to consumers and consumer rights, the attitudes of the European lawmaker and of the Court are similar. It is worth noting an attempt to standardize not only the term “durable medium” in the EU but also private law in the Draft of a Common Frame of Reference, in which art. I. – 1:106:(3) DCFR²⁰⁸ included proposal of a definition of a durable medium as any material on which information is stored so that it is accessible for future reference for a period of time adequate to the purposes of the information, and which allows the unchanged reproduction of this information.

Analyzing the above regulations, it must be stated that, as a rule, the definitions of a “durable medium” are consistent. In practice, there are small differences (e.g., such terms as: instrument, device or material), which mainly follows from the various periods in which they were introduced and from the conceptual framework used in the given legislative act, as well as from the absence of uniform terms related to cyberspace.

The main elements of the definitions, indicating the properties of a durable medium, are uniform and fixed in all of the above-mentioned definitions. These include: 1) the possibility to store information; 2) the possibility to recover stored information in an unchanged form; 3) durability, allowing unhindered access to the contents included therein at least for an adequate period of time, for the purposes for which the information thereon has been used.

The above review of definitions, and also judgments issued by the CJEU and practices applied, indicates a significant evolution of the term “durable medium”, as well as the notion of the document which should be provided under the above provisions. From a paper document and a traditional, physical, durable medium, through electronic documents on a physical durable medium (CD, DVD, etc.) to electronic documents and “dematerialized” digital media²⁰⁹ which was originally in “one place” (the uniform, physical location of a server) to a distributed recording and medium. Tech-

208 Draft of a Common Frame of Reference developed by the Study Group on a European Civil Code and the “Acquis Group” – European Research Group on Existing EC Private Law.

209 It is a sort of simplification, because a physical medium remains physical (servers, disks, etc.), but not necessarily under the control of the document’s addressee.

nological development has a significant effect on the understanding of the term of “durable medium”. A lot indicates the next stage will consist of blockchain technology.

When discussing the term “durable medium”, we should note the evolution of the term “document” to be provided using a durable medium. The definition of “electronic document” from the eIDAS Regulation is particularly significant and standardizing²¹⁰ – in point 35 of article 3 it states that an “electronic document” means any content stored in electronic form, in particular text or sound, visual or audiovisual recording²¹¹.

The issue of correct and practical implementation of “durable medium” is extremely important, taking into account the negative consequences, provided for in community provisions and their domestic implementations, related to financial, consumer and other regulations. That is why it is necessary to analyze the possibility to apply blockchain technology to meeting the requirements of a “durable medium”.

*Blockchain technology and durable media*²¹²

Despite the numerous pieces of legislation in which the term “durable medium” has been defined, that term should be considered uniform in the EU, which, to a considerable extent, results from judgments of the CJEU. A durable medium must perform the three basic functions indicated above. That is why the method of using the blockchain technology to meeting the “durable medium” requirements will be discussed “in abstraction”, without reference to particular legislation, indicating the properties that must be demonstrated.

The initial pilot programs and implementations demonstrate that proper implementation of the blockchain technology allows one to ensure the properties required by provisions of the law in terms of meeting the requirements of a durable medium. However, the application of blockchains alone is not sufficient. It is additionally necessary to introduce proper legal

210 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; L 257/73.

211 See also D. Szostek [in:] *Informatyzacja postępowania cywilnego*, ed. D. Szostek, J. Gołaczyński, Warsaw 2016, p. 69 et seq.

212 The issue described below may also apply to the construction of registers, ledgers, records, etc.

and organizational mechanisms, and to implement the system properly, especially considering that there are at least several methods of using the blockchain technology for meeting the requirements of a durable medium.

The whole process of meeting the requirements of the law by the entities bearing information obligations or the obligations to provide proper documents should be divided into the following processes: 1) preparing (generating) a document containing the contents required by provisions of the law (in the proper form required for the given activity²¹³), 2). securing it properly for the purpose of ensuring authenticity and integrity, 3) providing it effectively on a durable medium to the entitled person so as to allow a) storage of information on it; b) the possibility to recover the stored information in an unchanged form; c) durability so as to enable unhindered access to the contents stored for an adequate period of time, for the purpose for which the stored information should be used. This does not mean, however, that the entity obliged to provide a document on a durable medium is to lose the right to review it. In turn, they may not manipulate it, on their own delete it, change its contents or the document metadata, limit the access rights to the document, etc.

So far, in the “paper world”, in the case of the obligation to provide a document, there usually existed two counterparts thereof (the so-called original and a copy or two identical originals), one for each party. The piece of paper guaranteed the impossibility to change and the possibility to verify, in the case of claims of change, manipulation or forgery of a document. The blockchain technology is changing the way of functioning of block-recorded documents. Everyone entitled has the right to possess the register (and the data, to which it is entitled) based on the principle of sharing information. Therefore, “one” document is available to everyone entitled, recorded in a block, stored in a distributed manner by each person entitled. There are no “originals” or “copies”; there is document and access thereto, as well as the technological guarantee of its non-repudiation. On a piece of paper, authenticity and integrity are guaranteed by handwritten signatures (which, nowadays, are not difficult to copy and reuse). In an electronic document, that role is played by cryptographic protection. Proper application of blockchain technology is to guarantee a high level of cryptographic security of the document recorded in a block.

213 The issues of form exceed this study, which concentrates on the issue of using blockchain technology, its admissibility and the consequences of implementation.

Private or public blockchain as technology for durable media?

The contemporary digital trading makes use both of public and private blockchains. Because of legal regulations and obligations of EU entities towards consumers or recipients of financial services, as well as the legal system functioning in the EU, and the regulatory supervision over the financial sector, and the competition and consumer-rights supervision, it might seem that public blockchains are not advisable to be applied to a durable medium. It should be remembered that a public blockchain is fully open-source, within which everyone, without any personal or territorial limitation, may install suitable software on one's device and download the whole or any fragment of a database and, usually, make its "copy" available to other nodes. Operations within public blockchains usually do not require the consent of the ledger operators. However, this does not mean that it may not be used as a tool for meeting the legal requirements of a durable medium.

Use of private blockchains as technology for durable media

One of the proposals for effective provision of documents on a durable medium is use of the private blockchain technology available only to the entitled entity or entities which ensures confidentiality of the data included in the ledger to a higher degree.

The non-repudiation of a public blockchain consisting in its "democratization" and the need to obtain the consensus of all or a majority of the persons entitled to publish a document is not so necessary in the case of entities operating on a regulated market or in the case of entities operating under provisions of the law that bear liability for damages.

The non-repudiation and guarantee of Bitcoin consist in acceptance and consensus by many users and in cryptographic security by the "miners"²¹⁴. The non-repudiation and guarantee of authenticity of documents provided by the entities obliged to provide them on a durable medium result from provisions of the law, penal liability for making false statements or falsifying documents, civil liability (including for damages, in case of damage),

214 This does not mean that these persons do not bear legal liability. However, it is much more difficult to demonstrate, and even more difficult to adjudicate and enforce, taking into account the current "fledgling" stage of the legal aspects of Bitcoin.

as well as administrative liability before competent supervisory authorities. The blockchain technology “only” constitutes an additional technical and cybernetic security mechanism used for protecting those entities against violating the law and for proving effective provision of a document on a durable medium, and ensuring authenticity and integrity of the document provided.

In a private blockchain, the blockchain applied to the durable medium should be made available solely to entitled entities, upon prior consent of the system operator or operators (*permissioned blockchains*). Also, it should be managed by the ledger operator or, even better, operators. It is a very good idea to have multiple operators. That is because it allows a joining of consensus (on which a public blockchain is based) with a private blockchain, where approval of a record in a block may require the consensus of all, most or several operators (depending on the technical solution adopted). In the case of using the blockchain technology for provision of a durable medium by a single entrepreneur, usually that entrepreneur is the sole operator (e.g., for meeting the information obligation under consumer laws). In turn, in the case of a consortium (e.g., of banks), the optimum solution is consensus of multiple operators (e.g., of all the banks within the consortium or banks and technology provider). Such a solution makes protection not originate only from one provider of the service, but is secured with a network of nodes being controlled by various entities participating in the network. When using a private blockchain, blocks may be used for publishing whole documents or only hashes thereof.

Use of public blockchains as technology for durable media

There are many arguments for applying private blockchains as technology for meeting the requirements of a durable medium. However, the benefits of using blockchain technology are not always fully used, particularly if there is only one operator managing all the nodes. Although data is recorded in blocks, the same entity provides verification and acceptance services (which, as such, is not bad and meets the requirements of a durable medium).

An alternative solution to private a blockchain is the use of the benefits and non-repudiation of a public blockchain. It is possible to use it as a durable medium by publishing, in the blocks, not the whole documents provided, but hashes thereof, while recording the documents themselves in an external repository (archive) together with the hashes thereof. The

archive contains documents and hashes, and the blockchain – only the hash that allows the verification of the authenticity and integrity of the document recorded in the archive. Any change, modification or attempt at deletion is always detectable by comparing the document hash with the hash recorded in the blockchain.

Ways of recording documents on durable media

An important issue for meeting the requirements of a “durable medium” is specifying the method, or rather the “place”, or recording the data making up the document in the blocks, i.e., archiving it. It would be difficult to indicate a “place” in the traditional meaning of that word, because the process consists of recording (archiving) with the use of a computational cloud, in a distributed manner. The optimum solution would be to record the ledger with all the participants in the blockchain network, in their archives or repositories (servers), by means of DLT. This guarantees security of data recording, and makes hacking attacks significantly more difficult (an attack would have to take place at the same time on all the nodes). Also, it facilitates node recovery in case of data loss. However, it is not always possible, and in the case of using private blockchain technology – not advisable.

Another solution is storing the data in one location (an archive or repository). Such a situation takes place, for example, when it is one entity that uses blockchain technology. Recordings may be stored either on its servers or on the servers of the blockchain-technology service provider (an external archive), or both. From the point of view of a “durable medium”, it would be more beneficial to use several repositories. First, blockchain technology is based on data recordings grouped in blocks in multiple nodes (the more the better). Second, the more locations of block recording and network nodes there are, the higher the security is. Furthermore, an external archive allows one to meet the requirements of a durable medium indicated in CJEU judgments. Regardless of the archive location, data recording should take place using DLT (distributed ledger technology), ensuring integrity of the documents recorded. If a durable medium is established in a consortium, where many entities make use of the medium, with multiple nodes and “locations” of data recording grouped in blocks, the requirement of availability is fully met. In the case of one participant, in order to take into account judgment C-375-15 or the proceedings conducted in Poland by the President of the Office for Competition and Consumer Protection

(protecting against, among others, bank practices and publication of the information required by the act on electronic payments solely in their ICT system), it is necessary to provide an additional, external archive, either by the blockchain service provider or by another entity. In theory, one may indicate the solution where not only the consortium participants and service provider or another entity providing the external archive service store the data recorded in the blockchain, but the ledgers might be recorded by each entity obtaining a document on a durable medium, while access would be provided solely to the documents to which they are entitled (ensured through proper encryption and access policy), without the possibility to access others. Such a solution, although legal and meeting all the requirements indicated in the quoted judgment by the CJEU, and technologically possible (applied, for example, in Bitcoin, where everyone may download the whole ledger), does not seem practical, for example due to the potential size of the ledgers that need to be downloaded and archived, due to energy consumption of the process and the factual lack of need on the part of the client.

To sum up, in the blockchain technology, in particular in its open-source version, there are various possible ways of archiving documents to meet the requirements of a durable medium and ensure document authenticity and integrity, and to allow subsequent verification of authenticity of the document data and metadata. Blockchain blocks may be used to record the whole document. We then deal with its full verifiability, certainty of authenticity and integrity. The characteristics of an archive based on DLT with archiving of whole documents consist of a lack of the possibility to delete or change the object logs, i.e., the documents recorded or the information on them. It completely meets the requirements of a durable medium, i.e., invariability of the information provided.

Another solution is publishing a document and archiving it in a repository or several repositories with simultaneous recording, in a (private or public) blockchain, of information on the published document together with the result of its hash function. In that variant, the document itself is not recorded in a blockchain. The application of a blockchain-based data register ensures that the value of a hash function of a published document that is recorded may not be removed from the register. That property allows a client of a bank or a consumer, to whom the information is provided on a durable medium, to verify whether the form of the hash function for the document that has been provided to them has the same form as the one that was recorded during document publication. If both values are the same, it means that the document has not been amended after publication.

Technical modification of the document is possible then, but easy to detect (by comparing the hashes). A modified document will no longer have the same hash as the document recorded in a block. The solution described guarantees the possibility to verify document authenticity and integrity and meets the requirements of a durable medium.

“Forgetting” a document on a durable medium

Under a judgment issued by the CJEU, documents provided on a durable medium should be available so as to allow access to them and copy them in an unchanged form for an adequate period of time without the possibility for the provider or another entity to amend the contents thereof unilaterally. The blockchain technology offers such a functionality. What is important is that in case of recording the whole document in a block, the document is irremovable.

However, it is possible to “forget” it. Access to the given document in a block ledger takes place through cryptography that only allows authorized entities to read the document. Forgetting consists of destroying the cryptographic data that allows one to become familiar with the document, and thus making it impossible for anyone to read it. To meet the requirements included in the CJEU judgment, a durable medium must either completely exclude the possibility of “forgetting” (through proper cipher generation) or only allow the document addressee (or the addressee together with another entity, e.g., the bank) to “forget” it (by generating proper keys).

What is important is that in the case of forgetting, the blockchain ledger will keep the metadata which constitutes evidence that the document has existed, but its contents are then no longer available for any party.

“Providing” a document on a blockchain-based durable medium.

Contemporary technology is significantly changing the ways of providing documents. The previous physical transmission of control over a document (as in the case of a paper document) is being replaced by providing “access” to a document that does not exist physically and is only recorded in a cloud in digital form and cryptographically secured. The way of providing access logins (passwords) is also important for a durable medium. Under the judgment of the CJEU, only *“active behaviour on the part of the provider aimed at drawing the user’s attention to the existence and availability*

of that information” meets the requirement of correct provision of information to the client, without the need for its active behavior, e.g., when entering a website of a bank or of another entity providing a document on a durable medium. The way of providing the login is an element of the organization and processes of the work of the provider of documents in a durable medium and usually follows from a contract or from the regulations applicable to the parties. For example, a login to the document may be sent by email, text message or in a different way. Access to the document ensured also in the case of termination of the basic contract with the client (whose contract provided the basis for the obligation to provide information on a durable medium). From the point of view of the law, access to a document recorded on a durable medium should be treated, in the case of expiry of the basic contract, as an innominate contract separate from the basic one. It may be concluded directly with the provider, but also with a consortium or with the operator providing the software. The term of the access contract should be at least equal to the period of limitation of the claim resulting from the original contract, unless the provisions of the law provide otherwise.

The issue of evidence is also important for the entity providing information on a durable medium, for its integrity and authenticity before court or administrative authorities, in the case of court or administrative proceedings. In the lack of change of civil or administrative procedure in terms of legal presumptions, the application of the blockchain technology makes the evidence process become subject to the general rules for evidence, and thus it is the entity providing a document on a durable medium that is obliged to prove its authenticity and integrity (“originality”). However, before a document is recorded in a blockchain, it may be marked with a qualified electronic stamp or a qualified electronic signature as defined in the eIDAS Regulation, thus obtaining presumption of authenticity and integrity of the document. Such a double security mechanism (using eIDAS and blockchain tools) is not required for technological purposes, but is very beneficial in legal terms for the entity providing a document on a durable medium.

Chapter V. “Smart Contracts”.

Introduction

Development²¹⁵ of so-called “smart contracts” has taken place in recent years, and is associated with development of blockchain technology and its use for “smart contracts”. The concept of a smart contract, however, appeared long before blockchain technology – it was described over 10 years ago, in 1997, by Nick Szabo in his publication: Formalizing and Securing Relationships on Public Networks. (Szabo, 1997 Nr 9). The author believes that

“digital revolution challenges us to develop new institutions in a much shorter period of time. By extracting from our current laws, procedures, and theories those principles which remain applicable in cyberspace, we can retain much of this deep tradition, and greatly shorten the time needed to develop useful digital institutions. Computers make possible the running of algorithms heretofore prohibitively costly, and networks the quicker transmission of larger and more sophisticated messages. Furthermore, computer scientists and cryptographers have recently discovered many new and quite interesting algorithms. Combining these messages and algorithms makes possible a wide variety of new protocols. These protocols, running on public networks such as the Internet, both challenge and enable us to formalize and secure new kinds of relationships in this new environment, just as contract law, business forms, and accounting controls have long formalized and secured business relationships in the paper-based world. Smart contracts reduce mental and computational transaction costs imposed by either principals, third parties, or their tools. The contractual phases of search, negotiation, commitment, performance, and adjudication constitute the realm of smart contracts. Smart contracts utilize protocols and user interfaces to facilitate all steps of the contracting process. This gives us new ways to formalize and secure digital rela-

215 Due to the framework of this monograph, it does not cover all the issues of “smart contracts”, which should be addressed in a separate, in-depth dissertation.

tionships which are far more functional than their inanimate paper-based ancestors”²¹⁶.

The author indicates that new technologies have been used for concluding contracts for many years. At first, these were simple contracts being, in a way, the electronic equivalent of paper contracts that developed into “Electronic Data Interchange” (EDI)[, which] is the computer-to-computer communication of standardized business transactions between organizations, in a standard format that permits the receiver to perform the intended transaction. It renders traditional static business forms in cyberspace, and maintains the dependence on traditional controls. Beyond simple encryption and integrity checks, EDI does not take advantage of algorithms and protocols to add security and “smarts” to business relationships. It enables more rapid execution of traditional negotiation and performance-monitoring procedure. EDI loses some security features provided by physical paper (such as difficulty of copying) while not gaining advantages from the wide variety of protocols possible beyond simple message-passing of static forms. EDI contracts tend to be merely reiterations of existing terms and conditions, with only some timing expectations changed for the electronic environment. By redesigning our business relationships to take advantage of a richer set of protocols, smart contracts can take us far beyond the paper-based paradigm of shipping around forms in a secure manner”²¹⁷.

“Smart contracts” constitute the next stage of development of contracts online. Thus introducing cryptography as well as automaticity of processes and the possibility to automatically “perform” a contract after the premises specified in the programming code, are satisfied. Another significant stage of development of “smart contracts” was the appearance of Bitcoin and blockchain technology, allowing irreversible (as a rule) recording of a “smart contract” in blocks, its strong cryptographic security, as well as the possibility of self-execution. Bitcoin is a classic example of a programmed and self-executing “smart contract”. The concepts of Bitcoin and distributed ledgers, but, in particular, the concept of a “democratic” system existing on the Internet only, not associated formally with any territory, resulted in the development of the concept of the so-called DAO (*Decentralised Autonomous Organisation*), i.e., a special form of “smart contract” functioning within a completely autonomous entity existing solely in digital space. The opinions that “smart contracts” will force the establishment of new legal

216 http://ojphi.org/ojs/index.php/fm/article/view/548/469#* of 17 November 2018.

217 http://ojphi.org/ojs/index.php/fm/article/view/548/469#* of 17 November 2018.

frameworks functioning in cyberspace, above the jurisdictions of the respective states, appear more and more often in the literature as well as discussions devoted to blockchains and “smart contracts”. The views that modern technologized contracts are soon going to replace lawyers, because e-contracts are going to be self-executing, are not so uncommon. Such far-reaching conclusions are difficult to accept at the current stage of development of “smart contracts”. A more specific analysis thereof indicates that, in legal terms, they are not as revolutionary as some might want them to seem²¹⁸, (Scherback, 2014) and in a suitable interpretation they are well within the current framework of legal concepts and, for now, do not require the introduction of new, revolutionary concepts of autonomous cyberspace law or *lex electronica*. However, it is a fact that a new discipline is developing among the lawyers who deal with law and cyberspace – “legal programming”; integration of IT with the discipline of law²¹⁹ (Scherback, Integrating Computer Science into Legal Discipline: The Rise of Legal Programming, 2014).

Definition of a Smart Contract

From the point of view of the doctrine

The term “smart contract” was described in 1997 by Nick Szabo as a combination of protocols with user interfaces for the purpose of formalizing and securing relationships in computer networks. The objectives and principles of designing those systems were to be based on legal principles, economic theories and the theory of credible and secure protocols. The basic idea of “smart contracts” is that many types of contractual clauses (such as securities, deposits, specification of ownership rights, etc.) may be installed in our equipment and software in such a way that it is costly to violate the contract (if needed – too costly) for the violator, or even impossible. The author also indicates that “smart contracts” cover all the stages associated

218 Sergii Scherback: How Should Bitcoin be Regulated, European Journal of Legal Studies Articles No. 7, pp. 45-91; <http://cadmus.eui.eu/bitstream/handle/1814/32273/183UK.pdf?sequence=1&isAllowed=y> of 17 September 2018.

219 S. Schrebak: Integrating Computer Science into Legal Discipline: The Rise of Legal Programming https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496094 of 17 September 2018.

with a contract: searching, negotiations, obligation and, particularly important – its performance.

“Smart contracts” were defined in the Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser (which introduced the term of DLT), prepared for the British government, where “smart contracts” were described as contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system. The potential benefits of smart contracts include low contracting, enforcement, and compliance costs. However, there was noted the significant risk of the possibility of reliance on the computing system²²⁰.

The latest literature devoted to the law and latest technologies has also attempted to define that term. Merit Kolvart, Margus Poola and Addi Rull define “smart contracts” as smart, electronic “agents”; being a computer program capable of making a decision if certain preliminary conditions are met. At the same time, the authors were correct to note that the term “smart contracts” is understood differently by representatives of different fields. IT specialists consider smart contracts to be automatized solutions replacing traditional contracts, functioning in cyberspace without any jurisdiction and without the need to refer to any applicable laws. However, that statement seems to be too simplified, because, in legal terms, the character of the given “smart contract” is going to depend on multiple factors, and thus one may not assume a priori that it does not constitute a contract, even though expressed in a peculiar manner. That is because for lawyers, “smart contracts” are automatized agreements containing legal contracts, because it is impossible to avoid jurisdiction²²¹. (Kolvart, Margus and Addi, 2016)

In their online publication entitled *Legal Engineering on the Blockchain: ‘Smart Contracts’ as Legal Conduct*²²² (Goldenfine and Leiter, 2018), Jake Goldenfine and Andrea Leiter noted that automated transactions on the internet are part of everyday life for many people. An automated transaction can be thought of as a means of exchanging value in which some di-

220 <http://fintechpoland.com/wp-content/uploads/2017/01/Technologie-rozpoznanych-rejestrow-UK-GOfS-FTP-NASK-PL-1.pdf> of 17 July 2018.

221 Merit Koolvart, Margus Poola, Addi Rull: Smart Contracts [in]: *The Future of Law and eTechnologies*, ed. T. Kerikmae; A. Rull; Heidelberg, New York, London 2016r. pp. 134-136.

222 The material may be downloaded from the source https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3176363 of 18 August 2018.

mension of the actual exchange is processed by a machine, without human intervention. However, the relationship between the computational mechanism that processes the exchange, and the natural language contract that constitutes the agreement is not always clear (like in the case of Bitcoin – own remark). Smart contracts complicate this further because they are capable of more than simply processing payments. Technicians make use of technical standards and try to fill them with legal principles that demonstrate the character of standards. The authors believe that in any particular domain standards constitute a mosaic of rules that form the discrete regulatory modules (e.g., ISO – own remark) to which private agreements refer (e.g., by referring to a standard or a norm). As regulatory modules, they structure patterns of action and behavior into translatable packages that define the criteria for both technical interaction and legal transaction. The developing ecosystem is currently produced by various kinds of private entities that provide the computational modules for law-enforcement systems, while “standardizing” legal principles. In other words, it is development of legal regulations in technical architecture (by developing libraries of machine-readable transaction modules that correspond to traditional contracts), so as to facilitate enforcement of laws. That process may be called legal engineering (Goldenfine and Leiter, 2018).

Guido Governatori, Florian Idelberger, Zoran Milosevic, Regis Riveret, Giovanni Sartor and Xiwei Xu believe that a “smart contract” is any self-executing program operating in the environment of a distributed ledger, in particular in blockchain technology, aimed at ensuring the parties implement and perform the automated transaction. The performance may take place on the basis of records in software or result from external activities (Guido Governatori, 2018).

A concise but correct definition was suggested by A. Sherborn²²³ who defined “smart contracts” as automatically executed contracts bound by computer protocol, written in code, which automatically execute programmed functions in response to certain conditions being fulfilled. He notes that this concept is not novel, but with the integration of blockchain technology, “smart contracts” have the potential to automate and guarantee the performance of a great variety of obligations without the need for a central authority, legal system, or external enforcement mechanism. In these cases, smart contracts bring clarity, predictability, auditability, and

223 A. Sherborne: Blockchain, smart contracts and lawyer, <https://www.ibanet.org/Document/Default.aspx?DocumentUid=17badeaa-072a-403b-b63c-8fb-d985d198b>.

ease of enforcement to contractual relations while mitigating the risks associated with human involvement (Sherborne, 2017).

Legal point of view

The definition of “smart contracts” does not only function in theoretical or doctrinal deliberations on their essence. They have all been functioning for a relatively short period of time and, as the literature has suggested, they are at a preliminary stage of development. Their huge potential has been noticed and so they have been introduced in legal regulations. They are not only a *de lege ferenda* postulate, but also actually implemented laws.

An example may be amendment to statute 44 of chapter 26 of the Arizona States, by adding art. 5 concerning electronic transactions²²⁴, under which "SMART CONTRACT" MEANS AN EVENT-DRIVEN PROGRAM, WITH STATE, THAT RUNS ON A DISTRIBUTED, DECENTRALIZED, SHARED AND REPLICATED LEDGER AND THAT CAN TAKE CUSTODY OVER AND INSTRUCT TRANSFER OF ASSETS ON THAT LEDGER

and one may not claim it has no legal effects, validity or enforceability solely because it contains “smart instructions”. Furthermore, regardless of other regulations, it is considered that the data secured using blockchain technology is equivalent to other data, secured in other ways. That principle applies to ownership-transfer contracts or contracts for use.

The definition of a “smart contract” was also included in Decree of the President of the Republic of Belarus No. 8 of December 21, 2017, annex No. 1 on Development of Digital Economy²²⁵ – program code²²⁶ intended for functioning in the transaction block ledger (blockchain), another distributed-information system for purposes of automated performance and/or execution of transactions or performance of other legally significant actions.

224 Bill Text AZ (Arizona House Bill) HB2417 of 2017. See <https://legiscan.com/AZ/text/HB2417/id/1497439>.

225 <http://law.by/document/?guid=3871&cp0=Pd1700008e> of 17 July 2018.

226 Many definitions use the term “code”. It was defined by S. Schrebak: Integrating Computer Science into Legal Discipline: The Rise of Legal Programming https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496094 of 17 July 2018. Code is software that allows the computers’ functioning, interconnectedness and interaction. Put it more simply, everything that one sees on the Internet is delivered by means of code.

The latest European regulations that include definitions of smart contracts are the Maltese acts regulating blockchains: Malta Digital Innovation Authority Act C901²²⁷ and Virtual Financial Asset Act C778²²⁸. Both introduced an identical definition: "smart contract" means a form of innovative technology arrangement consisting of: (a) a computer protocol; and, or (b) an agreement concluded wholly or partly in an electronic form which is automatable and enforceable by execution of computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both.

In the opinion of the author, that definition completely reflects the essence of a "smart contract" and may be considered a model.

"Smart contracts" are slowly becoming reality, one that is legally regulated. At lot indicates that, in the foreseeable future, other states in the world are also going to introduce proper regulations in that regard. That is why that issue is worth examining.

The Notion, Properties and Classification of "Smart Contracts"

Notion and properties

The term "smart contract" may be considered as not particularly accurate, because it does not really reflect its actual role or notion, often causing misunderstanding. In public statements, in particular those made by start-uppers, we often read that a "smart contract" replaces a contract, is not subject to any territorial jurisdiction and functions only online. That thesis is particularly wrong and expresses so-called wishful thinking²²⁹ (Rogers, Jones-Fenleigh and Sanitt, 2017).

The term "smart contract" is very non-uniform, both in literature and in practice, and covers a number of different events. Basic elements included in most definitions are: a record in programming code and self-execution or an automated method of execution. Sometimes, but not always, the ele-

227 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=1> of 11 November 2018.

228 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1> access of 11 November 2018.

229 J. Rogers, JH. Jones-Fenleigh, A. Sanitt: Arbitrating "smart contract" disputes [in:] International arbitration report, October 2017r. Northon Rose Fulbright <http://www.nortonrosefulbright.com/files/20170925-international-arbitration-report-issue-9-157156.pdf> of 20 July 2018. p. 22.

ments listed also include the need to record in a blockchain or in DLT. In practice, most “smart contracts” are recorded that way. That element is also indicated by the legal definitions presented above. However, the literature does not always indicate that element as decisive. There is also indicated the following element: recording in the code of modules containing contractual clauses or other functionalities, as well as their irrevocability²³⁰ (execution on account of recording in a program).

The word “contract” used in the notion described should be considered particularly unfortunate, as it suggests that, in each case, we are dealing with an agreement, which is not the case. “Smart contracts” are not always agreements, either in the legal or casual sense²³¹. In practice, “smart contracts” may be classified into two types: 1) an actual agreement, concluded solely online, through its acceptance (but often also, additionally, by downloading software), that is “self-executing” – an example of such an agreement is an agreement among miners for mining Bitcoin; 2) a tool (medium) of record (usually in a blockchain) reflecting an agreement concluded before and in a traditional way (e.g., on paper or in the form of a document), often being a framework or conditional agreement, the performance of which (i.e., in programming terms, by launching further processes) by the program is automatic. From such a point of view, a “smart contract” is not always an agreement, but rather a tool that reflects it and facilitates its execution. The term “smart contract” should only be used in the former case. For that reason, in this study that term is written in inverted commas, to emphasize a certain autonomous term, not as an agreement in the legal sense. In legal definitions, “smart contracts” are defined as a program or programming code, i.e., as the technological tools that allow one to either (a) conclude an agreement and execute it automatically in part or in full or b) only execute it automatically completely or partly, while it is recorded in DLT or a blockchain, using a technique that guarantees authenticity and integrity as well as non-repudiation (not so much of the agreement, but rather of the record). All in all, what a “smart contract” is, is determined by its contents or the contents of the agreement that is the basis for launching it.

A “smart contract”, or actually the agreement that determines it, does not function in a legal vacuum, or outside of the law, or by replacing the

230 See also below.

231 As presented in A. Sherborne: Blockchain, Smart contracts and lawyer, p. 5 <https://www.ibanet.org/Document/Default.aspx?DocumentU-id=17badeaa-072a-403b-b63c-8fbd985d198b>.

law. That is regardless of whether it is concluded in electronic form directly through the programming code that constitutes a smart contract, or in a traditional way. It is associated with such issues as legal capacity, capacity for acts in law, way of concluding (declaration of intent, form, causality or abstractness), contents of the agreement, abusive (prohibited) clauses, execution, expiry, invalidity, possibility to amend, etc. As well as the "classic" regulations associated with choice of applicable law and jurisdiction, and in the lack of choice – allowing to search for them. Principles just like these referred to Bitcoin which is, in fact, a "smart contract". These issues refer to the classical interpretation of private law, and so this monograph is not the place for an in-depth examination.

In "smart contracts", the problem is not the agreement that is recorded or executed through this tool, but rather the technology that does not always allow synergy between the event resulting from legal regulations and operation of the program. Another problem may be anonymity of the entities (beneficiaries) concluding a contract in cyberspace. It is a much broader problem, as it not only refers to smart contracts, but also to other agreements concluded electronically, and it requires a separate discussion that exceeds the scope of this study.

The essence of a "smart contract" consists in its self-execution on the basis of permanent and, in fact, irremovable records in DLT or blockchain blocks. Depending on the type of blockchain, changes are currently either impossible (in case of applying a public blockchain of significant computing power), significantly hindered (in some private blockchains) or reversible (in case of some DLTs or private blockchains). This may result in a situation when, despite the appearance of the events justifying a lack of performance of an obligation under an agreement (e.g., a defect of a declaration of intent, absolute invalidity, suspended ineffectiveness, etc.), an obligation will be performed, including in case of a final and valid court judgment, and it will not be possible to "cease" its performance. However, such performance will bear a legal defect and be deprived of legal grounds, which also happens in traditionally performed agreements. Lawyers know the legal tools that allow the recovery of the condition which should appear on account of challenging an agreement²³². However, they are not al-

232 For example, when performance of a "smart contract" consists of making a payment, if the agreement is found invalid or challenged, the payment should be returned. If it is not returned voluntarily, it may be difficult to enforce it, especially if the agreement is international in character, or when the payment is made using cryptocurrencies.

ways effective or sufficient²³³. The situations is becoming seriously complicated not in legal terms, but rather in terms of potential recourse claims regarding “smart contracts”, where a number of entities are functioning, and one event causes the execution of another one (like in domino effect), where the impossibility to suspend performance of an agreement (e.g., with regard to the first event) may activate the subsequent one and so on.

Some say that the advantage of “smart contracts” is their non-repudiation and certainty of performance, and thus a lack of the necessity to enforce them before courts. Taking into account the legal regulations that apply nowadays, that statement resembles wishful thinking. Although an agreement is “self-executing”, this does not mean a lack of the possibility to challenge it and to pursue one’s claims before a court. In the countries, the procedures of which include presumption of correctness of the contents recorded in blockchains, it is easier to demonstrate the fact of conclusion of an agreement and to prove its contents, which does not result in the prohibition to pursue claims against the agreement itself²³⁴.

Classification

“Smart contracts” as well as the agreements associated with them are very diverse and impossible to classify unequivocally. The classifications vary depending on the criterion adopted.

In terms of the way of concluding an agreement connected with “smart contracts”, they can be classified into a) those concluded solely through the programming code included in the “smart contract”, b) those concluded solely in the traditional way (e.g., on paper or in the form of a document), c) hybrids, where the framework agreement associated with the “smart program” is concluded in a traditional way, while its details and special elements, in programming code, or an agreement is concluded in parallel in

233 When drawing up a “smart contract”, it is a good idea to allow the possibility to interfere with provisions and enforceability of the agreement, e.g., if the agreement is found invalid with a final and valid judgment.

234 Also in M.Kolvart, M. Poola, A. Rull, *Smart Contracts* [in:] *The Future of Law and eTechnologies*, ed. T. Kerikmae, A. Rull, Heidelberg, New York, London 2016r, p. 137 who believed that, in most cases of applying smart contracts, the parties may assume a lack of the need to enforce the contractual provisions before a court, which does not repeal jurisdiction or the right to pursue it in court.

the code and in the traditional way²³⁵. That classification is significant from the point of view of evidentiary proceedings before courts in case of a dispute. The programming code, through which an agreement is concluded (points a and c), is not always understandable for non-professionals²³⁶. The contents of an agreement is "embedded" in program modules which are filled in by the parties. There is usually no visualization of the agreement which is present when concluded in the traditional way. And the party/parties do not always realize the mechanism or manner of operation, or even the contents of the agreement. It is not a new situation, because agreements have been concluded online for many years, at first using passive forms, then active forms, when accepting and launching software, etc., without knowledge of the modules or principles of functioning. In "smart contracts", there is also recording in blockchains or DLT and self-execution of the agreement. When concluding an agreement through programming code, the parties submit declarations of intent in accordance with general principles of the law, with the principle of, for example, freedom of expression and of submitting declarations of intent. The fact that they express it through a program is of no relevance for assigning the effects of declarations of intent. The issue of using IT systems for submitting declarations of intent was described in detail almost 20 years ago (regarding, for example, programmed electronic mail or EDI), and "smart contracts", as a new, electronic medium, do not change anything in that regard (Szostek D. , *Czynność prawna a środki komunikacji elektronicznej*, 2004) (Beatge, 2002) (Wiebe, 2002) (Klam, 2002) (Heun, 1994) (Sussenberger, 47-49) (Koch, 1998). When using programming code for concluding an agreement, we have to take into account the risk of its defectiveness, of programming errors, software defects, risk associated with hacking attacks, etc., as seen in the example of the eDEO case²³⁷). Although smart contracts are to be certain and predictable as a rule, they remain exposed (like any software) to mistakes and errors in programming, which additionally increases the irre-

235 See also J. Rogers, H. Jones-Fenleigh, A. Sanitt: *Arbitrating Smart Contract Disputes*, p. 21 <http://www.nortonrosefulbright.com/files/20170925-international-arbitration-report-issue-9-157156.pdf> of 25 September 2018.

236 For an example of the functioning and programming of a "smart contract", see <https://www.youtube.com/watch?v=lQ4USRtzWko>.

237 David Siegel, 'Understanding the DAO Attack for Journalists' 19 June 2016 <<https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993>>.

versible character of blockchains²³⁸. A program recorded in a blockchain may not always be debugged (by finding and removing a defect from the software), and, despite the defect, the consequences of its self-execution may be serious and difficult (although not impossible from the legal point of view) to reverse. Programming errors may result in defective execution of a smart contract, there may appear discrepancies between the coded and traditional versions of an agreement, and they may function on the basis of inaccurate data²³⁹.

In terms of the structure of “smart contracts”, there are a) declared smart contracts and b) module smart contracts. The former appears in simple agreements, either bilateral or multilateral, where the whole contract is embedded in the code and is concluded in an adhesive way, i.e., by joining and accepting the whole, or a lack of the possibility to conclude a contract. An example of such a contract is an agreement among the miners in the Bitcoin system. A module “smart contract” allows a party to choose alternative, suitable modules that have been pre-programmed in the programming code. Although a party has freedom in choosing them, it may not change the contents or sequence of the modules. Its choice is limited to the options provided in advance in the system. Module smart contracts are used both for simple agreements and more complicated ones, including multilateral agreements.

In terms of the program language of the code, there are a) imperative and b) declarative “smart contracts”. Currently, most smart contracts assume an imperative approach, under which a “smart contract” directly specifies the computational operations which are to be executed for the purpose of executing the agreement. “When programming using an imperative language, the programmer records an explicit sequence of codes which are to be executed for the purpose of obtaining the intended result. The programmer must write what should be done and how. Declarative

-
- 238 A. Sherborne: Blockchain, smart contracts and lawyer, p. 6 https://www.google.com/url?sa=t&rcrt=j&q=&es-rc=s&source=web&cd=1&ved=0ahUKEwi_y9294qjCAhWMBi-wKHa3gCUMQFggvMAA&url=https%3A%2F%2Fwww.ibanet.org%2FDocument%2FDefault.aspx%3FDocumentUid%3D17badeaa-072a-403b-b63c-8fb-d985d198b&usq=AOvVaw1fDNjqMc9uJ2HdilGS44eI of 25 September 2018.
- 239 J. Rogers, H. Jones-Fenleigh, A. Sanitt: Arbitrating Smart Contract Disputes, p. 22; <http://www.nortonrosefulbright.com/files/20170925-international-arbitration-report-issue-9-157156.pdf> of 25 September 2018.

languages are an alternative to imperative languages²⁴⁰. Conventional algorithms may be analyzed, taking into account two components: the logical component which specifies what is to be done and the control component which specifies how it is to be done. The logical component is aimed at expressing the knowledge which may be used in the algorithm, while the control component only affects its effectiveness. As a result, when programming they have to record the exact sequence of steps to specify what to do. The programmer only describes what is to be done without specifying how to do it. Declarative smart contracts may be drawn up using various declarative languages, such as functional languages and logic-based languages²⁴¹ (Governatori and Inni, 2018).

As regards the criterion of the ecosystem, in which a “smart contract” functions, there exist the contracts: a) functioning in a closed ecosystem and b) with external sources that obtain additional data. The former are mainly based on an imperative programming language and all the functions, activities and events are decreed in the contract code. The “smart contracts” that refer to or make use of data from other sources (by obtaining them) are more complicated. They may be of referential character, may be obtained from a trusted third party (e.g., a court, public notary or trusted entity as defined in the EIDAS regulation) or from another entity.

In terms of the method of recording “smart contracts”: a) in DLT or b) in a blockchain. For both types of “smart contracts”, it is possible to use a number of different IT systems (public, private, etc.), as there are many DLT and blockchain systems.

Another criterion of classifying “smart contracts” is the way in which the agreement is executed. One of the properties of “smart contracts” is automaticity, or self-execution. However, the level of self-execution may be different. Contracts may be classified as a) completely self-executing or b) partly self-executing, in which, for full performance of obligations, additional activities are necessary, undertaken either by other software, devices or by another person/entity.

Using other criteria, “smart contracts” may be classified as a) self-destructing, i.e., when the code self-destructs after the obligation is performed or b) self-learning, i.e., based on the algorithms that are (or are similar to) artificial intelligence, making use of external sources for “learning”, or rather for changing the way of performing a contract on account of a change in

240 See also R. Kowalski: Algorithm=logic+control, Magazine Communications of the ACM, No. 22, July 1979 pp. 424-436.

241 <https://link.springer.com/article/10.1007%2Fs10506-018-9223-3> of 21 July 2018.

external sources (e.g., a change in the amount of interest results in a change in the way of performing the obligation).

In terms of access and possibility to conclude an agreement, “smart contracts” may be classified as

- a) open – available for an unlimited group of people (including foreign entities),
- b) partly open (e.g., for entities from a certain territory, e.g., the EU) or
- c) closed – for a specified group only. In terms of the number of parties to a smart contract:
 - a) bilateral or
 - b) multilateral.

In terms of subject of the agreement:

- a) those associated with the digital economy;
- b) those associated with traditional economy or
- c) hybrids.

These may include the contracts that use tokens or operate solely based on blockchain records without token transfers.

In terms of their cross-border character: a) international or b) domestic. In the former, it is necessary either to choose the law applicable to the contract or to look for it based on general principles of the law. In the latter, the law and jurisdiction are specified in advance, because of a lack of the cross-border element. In terms of the method of solving contract-related disputes: a) subject to arbitration or b) subject to procedures before traditional courts.

The above are just examples of classifications of “smart contracts”, and are not exhaustive. Their multiplicity, diversity as well as the possibility to apply many different criteria, do not allow a presentation of a complete and exhaustive classification.

Tokens in “smart contracts”.

Introduction

One of the tools used in “smart contracts” are tokens. They are not necessary for a “smart contract” to function, but over the last four years we have been witnessing tokenization of “smart contracts” and a growing tendency to trade in them in “cryptocurrency exchanges”. “Smart contracts” and tokens are used more and more often for collecting funds for initiatives related to blockchains and cryptocurrencies. An example is ICO (Initial Coin

Offering), referring to disposal of tokens in public offerings, usually in exchange for cryptocurrencies. Tokens, in particular those with a successful ICO, are usually listed in “cryptocurrency exchanges”, where initial buyers may dispose of them and new buyers may enter the exchange at any time. Depending on the type of agreement, tokens may play various roles. For example, it may (but does not have to) provide its holder with: access to services, but also the possibility to participate in a discussion, to address, for example, the issue of participating in a project (a classic example is the DAO project), but also the right to share in the profits or the right to the interest on the payment made in cryptocurrencies.

From a historical point of view, the first symbolic record related to disposal of tokens appeared in 2014, when seven projects generated the total amount of USD 30 million. The largest project of that time was the disposal of the tokens of eter – over 50 million eters were disposed of for over USD 18 million. The year 2015 was more peaceful: seven transactions generated a total of USD 9 million, including the largest one – Augur – which collected a little over 5 million dollars. The interest in tokens (on account of an increase in the value of Bitcoin) started to grow in 2016, when 43 companies, including Waves, Ionomi, Golem and Lisk, generated 256 million dollars. That sum included the infamous sale of chips in an independent investment fund, The DAO, the objective of which was to encourage development of the ecosystem by allowing investors to vote on which projects are to be financed. A little after the sale, over USD 150 million was collected, while a hacker stole (using a software loophole) tokens of the value of ca. 60 million dollars, which caused the project to collapse. A sudden explosion of interest in tokens took place in 2017 – 342 issues generated almost USD 5.4 billion and place that concept among the top innovations in blockchains. The decrease in the value of Bitcoin at the turn of 2017/2018 has not decreased the interest in tokens within ICO²⁴². In the first half of 2018, 150 projects disposed of tokens in exchange for USD 4.83 billion.

The concept of ICO, including tokens, thus became the most serious blockchain-using project, and the high amounts invested in the new tool demonstrate the size of that market and the place for “smart contracts”.

242 <https://www.coindesk.com/information/what-is-an-ico/> of 23 July 2018.

Definition

The term “token” is not new – it has been functioning for years in digital transactions as a security mechanism, in banking and in the qualified electronic signature PKI. It has recently adopted a new meaning, different than before, as well as new functions. As a result, completely different tools may be called tokens.

An earlier one – a generator of one-off codes, i.e., an electronic device (which may be in a “cloud” and use a dedicated app on a cell phone) used for authenticating online transactions, usually banking transactions. It consists of generating a sequence of digits using a unidirectional function based on two parameters – one permanent for the given device and another one, entered with a keyboard, from a monitor or generated based on time”²⁴³, a token, or one-time-password (OTP) generator. Regular tokens display variable codes, usually every 60 seconds. In banking, on account of the relatively high cost of generation, the tendency appeared to use a one-time code card (as used by banks several years ago) or to generate one-time text-message passwords.

The new meaning of the word “token” is significantly different from the previous one, and rather refers to the meaning resulting from direct translation from the English language, where “token” is a sign, symbol or evidence of something. That term is usually used in the phrase *digital token*.

Literature provides the following definition of token: a

“settlement unit generated in already existing blockchains. It is a digital representation of a unit of value issued by a private entity or institution, developed for independent management of its business model, so as to allow the users to interact with its products, as well as to facilitate and estimate the benefits among the parties interested. As tokens operate on the basis of blockchains, they may have all the properties of cryptocurrencies, as well as additional properties and functions e.g., self-destruction after use. They may play the role of chips, tickets, coupons, and even ballots”²⁴⁴.

The definition is not full, because there exist and are traded tokens not based on blockchains.

243 [https://pl.wikipedia.org/wiki/Token_\(generator_kodów\)](https://pl.wikipedia.org/wiki/Token_(generator_kodów)) of 26 June 2018.

244 M. Grzybowski, Sz. Bentyń: Kryptowaluty, p.277-278.

In terms of the issuer, tokens may be classified as embedded in a blockchain (native) or issued by the given entity (with or without a blockchain) for subsequent repurchase.

For the purposes of this study, a token shall be understood as a digital token based on blockchain technology.

While preparing this publication, the most popular token was one established on the Ethereum platform (Ethereum is both a cryptocurrency and an IT platform). Currently, the tokens that may be generated include: ERC-20 tokens and their extensions – ERC 223 and ERC-721. The Ethereum tokens include Utility Tokens and Security Tokens.

Utility Tokens provide access to services. They are usually used as means of payment for products or services (and may be usually obtained by ICO). These tokens are sometimes called "app coins" or "app tokens". *Security Tokens* reflect the balance of rights, ores or other financial or investment instruments²⁴⁵. It is indicated that they could also reflect shares in an enterprise or other entitlements. An example of a link between a share in a company and a token is the regulation of 30 May from the State of Vermont, described in more detail in chapter V.

The term "token" also has a legal definition in, among other places, Decree No. 8 of 2017 of the President of Belarus, under the annex to which a digital token is a record in a blockchain ledger or another distributed ledger (DLT), the purpose of which is verification of the right of the person holding a token to the given civil right and/or it is a cryptocurrency.

An interesting definition was suggested by the Maltese lawmakers in the Virtual Financial Asset Act C778²⁴⁶ of July 2018, under which "virtual token" means a form of digital medium recordation that has no utility, value or application outside of the DLT platform on which it was issued and may only be redeemed for funds on such platform directly by the issuer of such DLT asset: Provided that electronic money shall be excluded from this definition.

A token is nothing more than a record in a blockchain which may function within "smart contracts", but also outside of them. In the former case, it is one of the elements of a smart contract, and thus, following the *a maiori ad minus* principle, it should be treated (like smart contracts) as a

245 See also <http://antyweb.pl/ethereum-erc20-token/> of 26 June 2018.

246 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&cl=1> access of 11 November 2018.

technological tool²⁴⁷ in which the given entitlement of its holder is recorded under an agreement.

Tokens – legal issue

A token may be distributed under any type of “smart contract” or outside of them. Whenever we want to determine or attempt to indicate its legal character, we have to take into account a number of elements, among others the law applicable to the agreement, under which it is generated and disposed of, but also the contents of that agreement (taking into consideration the *ius cogens* and *ius dispositivum* provisions). It is not difficult to demonstrate applicable law in the case of ICO, because the entities that distribute tokens are usually real entities functioning in the real world, with real, physical seats²⁴⁸. A token is a tool and its function is determined by the laws applicable to it.

Therefore, in legal terms a token does not constitute some sort of revolutionary legal instrument unknown before. It is nothing more than a new medium of a legal instrument, which is indicated by the latest positions adopted by financial-supervision authorities, as seen in the report²⁴⁹ of the US Securities and Exchange Commission of 25 July 2017, in which it warns market participants that the offers and sale of digital assets (tokens) through “virtual” organizations managed by the organizations using DLT or block technologies, among others those described as ICO or “token sales”, are subject to the requirements of federal securities laws. Whether the given investment transaction includes offering or selling a security – regardless of the applied terminology or technology – depends on facts and circumstances, including on the economic realities of the given transaction. A report on an SEC investigation stated that the tokens offered and sold by the “virtual” organization called “DAO” constitute securities, and so are subject to federal securities laws. The report confirms that issuers of distributed securities or of the securities based on block technologies, must register the offers and sale of such securities, unless a valid exemption ap-

247 On how a token works and what its programming looks like: <https://www.ethereum.org/token> and <https://www.youtube.com/watch?v=jfFgecLL8UA> of 25 July 2018.

248 Attempts were made to distribute tokens on an anonymous basis, but without much success.

249 <https://www.sec.gov/litigation/investreport/34-81207.pdf>.

plies. The persons participating in unregistered offers may also incur liability for violating the provisions on trading in securities. Furthermore, stock exchanges, on which those securities are traded, must be registered, unless they are released from that obligation. The provisions of the federal act on trading in securities, associated with registration, are aimed at ensuring all the suitable information is obtained, and are subject to regulatory control for the purpose of protecting investors (COMMISSION, 2017).

Independently from the opinion of the US Securities and Exchange Commission, one week later, i.e., on 1 August, a similar position was adopted by the Monetary Authority of Singapore – MAS)²⁵⁰. It stated that the tokens offered or spent in Singapore will be regulated by the MAS if they meet the definition of the product specified in the act on securities. If digital tokens are covered by the definition of securities included in the SFA, issuers of such tokens will be obliged to submit and register a prospectus in the MAS system before offering such tokens, unless they are exempt. The issuers or intermediaries trading in such tokens would also be subject to the requirements regarding issuance of permits under the act on special financial arrangements and financial advisers, unless they are exempt, and to the applicable requirements regarding counteracting money laundering and the financing of terrorism. Furthermore, the platforms that facilitate secondary trading in such tokens would also have to be approved or acknowledged by the MAS, as an approved exchange or acknowledged market operator, accordingly. The digital tokens offered in Singapore and those offered in other countries are very different. Some offers may be subject to SFA, while others may not. All the issuers of digital tokens, intermediaries that facilitate or advise as regards offering digital tokens, and platforms that facilitate trading in digital tokens should, therefore, obtain independent legal advice in order to ensure their compliance with all the applicable provisions and, in certain cases, should consult with the MAS.

Europe has also paid attention (European Securities and Markets Authority²⁵¹ (ESMA) (Authority, 2017) and Polish Financial Supervision Authority (KNF)²⁵²) to the issue of trading in tokens and to the need for the

250 <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx> of 25 July 2018.

251 https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.

252 https://www.knf.gov.pl/o_nas/komunikaty?articleId=60178&cp_id=18.

entities functioning through ICO, whether they are or are not obliged to obtain a suitable permit for trading in them.

A very interesting regulation regarding trading in tokens was introduced in Belarus (it has been effective since 1 January 2018). Under the quoted Decree of the President of Belarus, legal persons are authorized to hold tokens and, taking into account the special properties specified in the decree, are entitled to create and publish their own tokens in the Republic of Belarus and abroad. They are also entitled to store tokens in virtual wallets, including with the use of cryptographic-platform operators, cryptocurrency-exchange operators, and to purchase, alienate tokens and to perform other transactions (operations) with their use.

Natural persons are entitled to hold tokens and, taking into account the special properties resulting from the decree: to acquire and store tokens in virtual wallets, to exchange tokens for other tokens, to purchase them, alienate them not only for Belarusian rubles but also for foreign currencies and electronic money, and to donate and transfer tokens. The activities consisting of mining, acquiring and alienating tokens, performed by natural persons without employing other natural persons under employment agreements and/or civil law agreements, do not constitute business activities. What is more, tokens do not have to be reported to state authorities. Cryptographic-platform operators and “cryptocurrency-exchange” operators are obliged to ensure availability on accounts in the banks of the Republic of Belarus of monetary means to the amount of not less than 1 million Belarusian rubles for a cryptographic-platform operator and not less than 200,000 Belarusian rubles for a “cryptocurrency-exchange” operator. A cryptographic-platform operator is entitled: to open accounts in banks and non-bank, credit-and-finance organizations in the Republic of Belarus and abroad for making settlements on trading and operations being carried out by them; to receive remuneration for services being rendered, including in tokens, to establish its amount and the order of collection from trading participants (customers); to perform (organize) transactions with residents and non-residents of the Republic of Belarus, aimed at placement of tokens, including abroad, acquisition and/or alienation of tokens for Belarusian rubles, foreign currency, electronic money, exchange of tokens for other tokens in the interests of customers or in own interests; to perform (organize) other transactions (operations) with tokens, with the exception of operations on the exchange of tokens for civil-right objects other than Belarusian rubles, foreign currency and electronic money. If the rights validated with a token are transferred to another person, it is enough to transfer the token to that person, except for the case of transfer of a right that

requires entry in state registers. A token transfer will be considered completed when the operation of transfer is reflected in the blockchain transaction ledger or in another distributed IT system based on the applicable principles (protocols). It is admissible to use tokens as remuneration for verification, to perform other operations in the transaction blockchain ledger or in another distributed ledger technology system. The projects in the scope of information and communication technologies, including with the use of transaction block ledger technology or DLT, may be executed under civil law partnership agreements.

The latest legal regulations in the world related to tokens and smart contracts is the Maltese Virtual Financial Assets (VFA) Act²⁵³ of 5 July 2018. In combination with two others (Innovative Technology Arrangements and Services Act²⁵⁴ and *Malta Digital Innovation Authority Act*²⁵⁵), that act regulates the manner of issuing tokens, state-authority supervision and protection of participants in token trading. However, as there are many types of tokens, a token may be considered not only a security or a financial instrument, but also a cryptocurrency or identification item.

The size and variety of tokens result in a situation when they will never meet the definition of securities or financial instruments. It is necessary to examine them each time from the legal point of view. Sometimes they will constitute cryptocurrencies, other times – identification items, used for the purposes similar to securities, i.e., embodying certain entitlements due to their holder, or solely for identification purposes, i.e., to entitle the given person to collect certain benefits. Their identification function²⁵⁶ (Machnikowski, *Kodeks cywilny. Komentarz*, 2016) consists of facilitating performance of obligations, including identification of the persons entitled. What is important is that in terms of identification items, the term “document” (being an identification item) should be interpreted broadly. It may be any material that allows the recording of certain characters on account of the new definition of the term document, not necessarily a tangible one.

To sum up, as a technological tool, in practice a token does not change a lot in legal terms, but constitutes an interesting and innovative implemen-

253 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1>, access on 8 November 2018.

254 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&l=1>, access on 8 November 2018.

255 <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=1>, access on 8 November 2018.

256 P. Machnikowski [in], *Kodeks cywilny. Komentarz*, Warsaw 2016, p. 1670.

tation of law in programming codes. It will be interesting to observe its development, as well as development of the legislation related to it.

“Smart contracts” as private law

“Smart contracts” and lawyers

Over the last twenty years, we have been witnessing an extremely fast development of technology as well as ICT systems. The development affects different sectors of the economy, thus producing a completely new one, i.e., a “digital” economy, supraterritorial and global in character. Even some lawyers are surprised by the character of some agreements, and of the law applicable to them, or to the location of data storage, not necessarily associated with the domicile of the persons concluding them.

The appearance and use of blockchains and establishment of “smart contracts” is the next stage of the above-mentioned development process. It is impossible for “smart contracts” to replace laws, or lawyers, but they will result in new specializations and competences. It would be impossible to stop the development of “smart contracts”, which streamline and facilitate business processes in many sectors, such as power or logistics, which is reflected in financial results. It should be remembered that they only constitute tools, not laws, and as tools, they are going to be developed while implementing laws, not replacing them. Since the very start of the development of new technologies, lawyers have been using IT tools that change the way they function, but also generate the demand for specialist knowledge and competences. The blockchain is just another stage of development – a difficult stage, because at present few lawyers deal with it, just as few lawyers dealt with the issues of using electronic mail or websites twenty years ago. The uses of new technologies in lawyers’ work may be divided into: a) using specialist online platforms and databases (of legislation, publications, judgments, etc.); b) using ICT tools for contacting clients, courts or administrative authorities (emails, electronic registry offices, video conferences, etc.) – put simply, quite often previous activities are performed in a digital form (an email is sent instead of a traditional letter); c) transferring data and resources to clouds and sharing resources with colleagues, and sharing data with clients using a cloud (those activities are being slow-

ly, but systematically, implemented and accepted by lawyers²⁵⁷); d) automating ²⁵⁸ the processes by using wizards, templates, automaticity in filling in data, e.g., based on xml (automation takes place at different levels and stages; right now it is usually partial and requires external sources, and often, also physical initiation by a person (currently, we are witnessing the initial phase of that development)); e) using DLT and blockchains as new ways of recording data (the initial stage or the start-up phase); f) using "smart-contract" tools for concluding or performing agreements (the initial stage or the start-up phase) and g) legal engineering²⁵⁹ – connecting legal regulations, as theses, with IT modules being program codes (implementation of legal provisions to programming codes (Furlog, 2012)) – that concept is at an experimental, pilot phase, executed within scientific research²⁶⁰. Each of these stages refers to a change or development of the

257 That process in the EU was significantly accelerate by issue of CCBE (Council of Bars and Law Societies of Europe) guidelines of 19 May 2017. See also D. Szostek (ed.): *Bezpieczeństwo danych i IT w Kancelarii prawnej*, Warsaw 2018 p. 303 et seq.

258 S. Schrebak : *Integrating Computer Science into Legal Discipline: The Rise of Legal Programming*, p. 7 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496094 of 22 July 2018.

259 See about law engineering: S. Schrebak : *Integrating Computer Science into Legal Discipline: The Rise of Legal Programming*, pp. 1-33 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496094 of 22 July 2018.

260 The development of legal engineering, just like the development of other types of expert systems, takes place in stages. Scientists assume different classifications of such stages. Developing the system of the code implementing legal regulations takes consists of the following stages: identification, i.e., describing what problems will be solved by the system, how and who will use it; conceptualization, ensuring formalization of lawyers' knowledge; prototyping, i.e., developing a prototype for initial testing purposes, identification and elimination of functional defects; development of the user interface; and testing and redefinition, which includes testing of the system. Expert systems are the systems that contain in-depth and rich knowledge at expert level in the given specialized field, functioning automatically. In law, they are called LES (Legal Expert Systems). They consist of the following elements: a database of knowledge representing the information used by the system in the process of solving problems; the mechanism of inference which, at different levels, consists of artificial intelligence or advanced algorithms that ensure interaction between the database of knowledge and the input data related to the problem which is to be solved, and presents the conclusions based on that interaction, as well as a user interface – the mechanism that ensures exchange of information with the user. See Jordan Furlong, 'The evolution of the legal services market: <http://www.law21.ca/2012/11/the-evolution-of-the-legal-services-market-stage-1/>, <http://www.law21.ca/>

tools used, but none of them will replace laws, even though they will affect laws and force adaptation to the changing reality and needs²⁶¹.

Custom, common law, *lex mercatoria*, arbitration and smart contracts

Nowadays, smart contracts are developed by private entities using so-called legal engineering, creating so-called ecosystems which, as indicated above, may take different forms, open, closed, functioning in a closed ecosystem or one that requires an additional source of data, etc. Closed smart contracts, functioning within one organization, usually subject to one jurisdiction, do not pose problems. A challenge is presented by the more and more popular smart contracts of a global character, functioning solely in cyberspace, for entities that function in different legal systems. The global character and tool of smart contracts significantly impacts agreement standardization, but also those laws applicable to them. The first chapters of this study indicate the significant impact of custom, standardization, and also technical norms, on the application of laws in cyberspace. It is possible, but not certain, that, in the foreseeable future, the regulations included in smart contracts will constitute legal references, like ISO norms for IT. And it is not so much production of some new norms, unknown before, but rather implementation of the already existing norms in programming codes, allowing them to be applied to a higher or lower degree. That is because the international trade of today already exists *lex mercatoria* (e.g. INCOTERMS) or standardized rules (e.g., UNIDROIT, PECL or DCFR) (Popiołek, 2013). Smart contracts may constitute the tool allowing them to be more easily applied together with any other rules, functioning today, regarding international agreements and interpretation thereof (e.g. within hybrid smart contracts).

The English literature (Goldenfine and Leiter, 2018) indicates that the activities of the private entities²⁶² that develop libraries of transaction mod-

2012/11/the-evolution-of-the-legal-services-market-stage-2/, <http://www.law21.ca/2012/11/the-evolution-of-the-legal-services-market-stage-3/> of 1 August 2018.

261 An example in Europe is consumer law which, at the beginning of its development, mainly referred to traditional ways of concluding agreements with a consumer, while it currently covers the whole of eCommerce and, to a growing degree, also the digital economy.

262 Such as: Enterprise Ethereum Alliance,⁴ Mattereum, Open Law (2017), Agrello (2017),⁵ the R3 Consortium (2018), Common Accord, and Legalese (2017–2018).

ules readable in a natural language, thus establishing the foundations for more complex transactions, which are more and more often implemented in smart contracts, demonstrate many common features with development of *lex mercatoria* in the Middle Ages, customs or common law. The authors indicate that the initial Medieval documents were “technical” artifacts connecting human conduct with enforcement of the law. They were not prepared by judges, but by lawyers (public notaries) who developed the standards of legal grounds. Firstly, common law determines and specifies which behaviors are good or bad, and secondly, it allows the indication of the behaviors that are reasonable and acceptable, and finally, it interferes and authoritatively determines the rules of conduct. The medieval common law was a dictionary-based system: the contents, basic principles as well as structure were specified, to a large degree, on the basis of entries of documents in a catalog. Those cataloged documents were, in a way, functioning as a library of acceptable transactions. It is argued that the decision on what conduct is legal or not depends on the proper and available records. (Goldenfine and Leiter, 2018). It is also worth noting the medieval *lex mercatoria*, “when transactions performed by merchants from different states were subject to standards of common law. At that time, there developed the autonomous laws of merchants, considered common laws. The cause for that was the practical necessity to establish a quick and secure system of laws for the classified exchange of goods for money or transportation. They applied in the fairs located and functioning in many European cities. At that time, merchants’ laws were supplemented with courts, the procedures of which resembled contemporary arbitration – the courts would resolve the disputes resulting from the agreements concluded at the markets. An important role was also performed by public notaries (lawyers) who legally shaped most agreements concluded in international trading²⁶³ (Fuchs, 2013) (Fuchs, *Lex mercatoria w międzynarodowym obrocie handlowym*, 2000).

Lawyer’s work consists of the ability to transfer reality to proper records in a document or a number of documents comprising a sort of register, so as to allow debt collection. In the Middle Ages there were agreements drawn up by public notaries, while nowadays agreements are drawn up by lawyers in cooperation with IT specialists in “smart contracts”. The analogy

263 B. Fuchs: *Lex mercatoria-term* [in:] *System prawa handlowego*. Vol. 9, *Międzynarodowe Prawo Handlowe*, ed. W. Popiołek, Warsaw 2013, pp. 47-50; B. Fuchs: *Lex mercatoria w międzynarodowym obrocie handlowym*. Kraków 2000, p. 21 et seq.

to *lex mercatoria* from the Middle Ages is very visible, with the reservation that bartering from the past was replaced with “smart contract” ecosystems. Despite the passing of one thousand years, the issue of a lack of regulations (this time regarding the global digital economy), is solved in a similar way, especially that supranational arbitration constitutes the optimum method, often used in trans-border agreements within “smart contracts”, (Sherborne A.) instead of domestic courts (allowing the possibility to overcome the issues with selection of the law and specialization of the arbitrators), the decisions of which are enforceable in domestic jurisdiction under the New York Convention (Goldenfine and Leiter, 2018). The issue is open as to whether the agreements within smart contracts will be subject to specialized authorities (arbitrations) which may also function online or, as is the current case, traditional arbitrations. Probably, arbitration is going to become, for many reasons, the preferred method of solving disputes related to smart contracts, and the disputes related to smart contracts will, in turn, lead to innovations in arbitration, because through the laws and procedures of arbitration the arbitration authorities will adapt to the needs resulting from the new types of disputes.

As some disputes related to “smart contracts” may be associated with evidence for existence of computer equipment and/or software, and there is the risk of disclosure of confidential information on source code, which may have serious commercial consequences for one or both parties, is better to agree that the disputes will be resolved through confidential arbitration and to limit disclosure of information. Some disputes related to “smart contracts” will be the disputes regarding laws and agreements, but others will be highly technical in character, for example if modules do not function according to expectations. It may be presumed that arbitration courts will probably, in time, establish groups of specialized arbiters with suitable experience, and will publish procedures adapted to the needs of the respective groups and types of “smart contracts”²⁶⁴ (Rogers, Jones-Fenleigh and Sanitt, 2017).

264 J. Rogers, JH. Jones-Fenleigh, A. Sanitt: Arbitrating “smart contract” disputes [in:] International arbitration report, October 2017r. Norton Rose Fulbright <http://www.nortonrosefulbright.com/files/20170925-international-arbitration-report-issue-9-157156.pdf> of 23 September 2018. p. 23.

Chapter VI. The future of blockchain solutions in legal regulations (an initiated discussion).

Blockchain technology has become familiar in business transactions, both in the traditional and digital economy. As shown at the beginning of this monograph, more and more states, consortia and single institutions are implementing and using the opportunities related to the new tool. Also, the initial legal chaos or problem with applying legal regulations to the blockchain and new tools are slowly being eliminated by explicit decisions made by supervisory authorities, by connection of the new tools with domestic law or with the principles of looking for applicable law and jurisdiction. What is also important is the development of international arbitration related to ICO, “smart contracts”, tokens or cryptocurrencies. The pace of activities with regard to blockchains, just like the pace of development of technology, is extremely high. While this monograph was being written, a number of changes and initiatives appeared which, as far as possible, were included herein. The most interesting ones include the adoption (30 May 2018) and the coming into effect (1 July 2018) of the first act in the world devoted to blockchain technology and the introduction (in response to the problem of DAO) of the first blockchain-based limited-liability company that functions solely on a virtual basis.

On 30 May in the state of Vermont (USA), Governor Phil Scott signed the Act Related to Blockchain Business Development, the objective of which is to consolidate the position of the state of Vermont as the leader of supporting the initiatives related to blockchain technology. The new tasks of the Agency of Commerce and Community Development include promotion and development of business support programs for 1) the business private sector related to blockchain technologies, including blockchains for banking, insurance, retail and services as well as cryptocurrencies; 2) analyzing and amending the legal mechanisms and regulations to allow and support implementation of blockchain technologies in public and private areas and 3) educating and training employees in the scope of blockchain technology, blockchains in finance and in related fields. In order to achieve this, Sec. 7.11 VSA was amended in that a new type of company was added to subchapter 12 in chapter 25: a Blockchain-Based Limited-Liability Company (BLLC). The act introduces a number of definitions, such as: a “blockchain”, which means a mathematically secured,

chronological and decentralized register or database, whether it is managed using an online peer-to-peer network or in another way; “blockchain technology”, i.e., computer software or computer equipment, or groups of computer software or computer equipment, or both types of software and equipment, which use or allow the operation of blockchains; “participant”, i.e., a) any person holding a partial or full copy of the decentralized consensus ledger or database used within the blockchain or who otherwise participates in the processes of approving such a book or database, b) any person controlling any digital resources in blockchain technology; and c) any person who has a significant contribution to protocols. “Protocols” are understood as certain regulatory models of the software which regulates the principles, operations and communication among the network nodes used by the users; and, finally, “virtual currency”, which means a digital representation of value: a) used as a means of exchange, settlement unit or to store value; and b) not being legal tender, whether it is denominated as legal tender or not.

A limited-liability company operating on the basis of blockchains may be established under the provisions of § 4172 for the purpose of conducting business activities based on blockchain technology, but its statute must clearly indicate that it operates as a BLLC and that it meets the legal requirements specified in the act. No existing regulations associated with companies allow the management of a BLLC, in full or in part, using blockchain technology. The articles of association of the company have to include the abridged objective and mission of the BLLC; indication whether a decentralized consensus ledger or database, used or activated through the BLLC, will be fully or partly decentralized, and whether such a ledger or database will be fully or partly public or private, including the scope of access of participants to information and permits for reviewing and recording data in protocols; the voting procedure which may also include the “smart contracts” executed using blockchain technology; the proposed managers, members as well as other groups of participants in the BLLC being entitled to update or modify the software protocols or systems or both these elements; and the way of adopting other amendments to the articles of association of the BLLC as well as any other issues related to management and operation within the BLLC. Furthermore, they must include the principles of adopting protocols, reacting to system security violations or other, unauthorized activities affecting the integrity of the blockchain technology used in the BLLC; specify the way of becoming a member of or obtaining shares in the BLLC, which may be expressed in the form of participation units, shares in share capital or other forms of

participation in profits; and specify the rights and obligations of each group of participants in the BLLC, including which participants have the rights and obligations of shareholders and to manage.

A member or manager of a BLLC may interact with a BLLC in many roles, including as a member, manager, developer, node, miner or another participant in a BLLC, or as an entrepreneur and holder of a currency for its own account or for the account of other persons, on the condition that such a member or manager complies with any and all the trust obligations specified by the law. The activities of a member or manager who cooperates with BLLC by performing several roles are not considered conducted in the state of the BLLC merely because the BLLC is incorporated in that state.

Also, there was introduced the regulation on the manner of reaching consensus which, in a BLLC, may 1) include any and all the reasonable algorithm measures for the purpose of reaching consensus in the process of validation of records, as well as of the requirements, processes and procedures of operations or making organizational decisions regarding the blockchain technology used by the BLLC; and 2) under the procedure specified in section 4173 of the act – modify the consensual procedures, processes and requirements or replace the consensual procedures, requirements and processes which are consistent with legal requirements and provisions on management of BLLCs, into new processes.

Unless explicitly provided otherwise, the act does not release a BLLC from any other provisions, be they statutory or implementing provisions of the law of the State of Vermont or of federal law, including state and federal securities laws. Except for the special provisions on BLLCs, they are subject to the provisions of the Limited Liability Company Act of the State of Vermont.

At the same time, the Vermont State Archives and Records Administration, in collaboration with Vermont League of Cities and Towns, Vermont Municipal Clerks' and Treasurers' Association, and Agency of Digital Services were obliged to assess blockchain technology until 15 January 2019 for the purpose of systematic and effective management of public registers and to adopt the provisions necessary for supporting blockchain technology, including to make entries in the land registry²⁶⁵.

265 See <https://legislature.vermont.gov/assets/Documents/2018/Docs/BILLS/S-0269/S-0269%20As%20passed%20by%20the%20Senate%20Official.pdf> of 25 July 2018.

A number of publications and reports demonstrate many ways of using blockchains, in many disciplines, such as: finance, insurance, power, logistics, securities, state and public registers, but also copyrights, digital content, parliamentary voting, referenda and others. Some of them require modification of the previous regulations, while others may be introduced without significant changes. In any case, nowadays there is no need to create new, supraterritorial cyberspace to regulate the issues of cryptocurrencies or blockchains. In turn, it is necessary to notice the new technology with its associated problems and to adapt legal regulations properly and, in particular, to interpret the current provisions of the law properly.

The blockchain is the next stage of evolution of the tools used in the law, not a legal revolution. It is a tool, in which the legal concepts and theories that are several hundred years old continue to apply.

The fact that the European Union noticed the potential of blockchains should be considered a significant event that will result in greater involvement of the Community in the activities related to that technology. What seems necessary is a comprehensive legal regulation of the European and domestic regulations, the purpose of which would be to make best use of that technology, the potential of which, it seems, highly exceeds the previous implementations and will significantly, as the next stage of digital evolution, impact the way of recording data, evidentiary process, etc. As a technology, the blockchain may solve a number of existing technical and legal issues. However, it generates a number of new ones. A lot, including the resources invested in blockchains, but also the size of pilot implementations, indicates that the blockchain is not just one of many technology-related fads of recent years. This publication is aimed at presenting the issue, but mainly to perceive it from the point of view of the law and a lawyer, which are often different from the points of view of IT specialists, economists or entrepreneurs. It does not assess the feasibility of introducing the blockchain technology in the respective areas of functioning of society, the state or business, but constitutes an attempt to explain the basic legal rules associated with it and to answer the question:

“Is the blockchain a revolution or “just” another stage of evolution of development of the digital economy, and what is its impact on the previously applicable principles, rules and provisions of the law?”

We will soon answer that.

Appendix

European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP))

The European Parliament,

- having regard to the question to the Commission on distributed ledger technologies and blockchains: building trust with disintermediation (O-000092/2018 – B8-0405/2018),
 - having regard to the motion for a resolution of the Committee on Industry, Research and Energy,
 - having regard to its resolution of 26 May 2016 on virtual currencies(1),
 - having regard to its resolution of 28 April 2017 on ‘FinTech: the influence of technology on the future of the financial sector’(2),
 - having regard to its resolution of 6 February 2018 on ‘Geo-blocking and other forms of discrimination based on customers’ nationality, place of residence or place of establishment’(3),
 - having regard to the General Data Protection Regulation (Regulation (EU) 2016/679),
 - having regard to the proposal for a regulation on extension of the duration of the European Fund for Strategic Investments (COM(2016)0597 – C8–0375/2016–2016/0276(COD)),
 - having regard to its resolution of 11 October 2017 on the Council position on the draft general budget of the European Union for the financial year 2018 (11815/2017 – C8–0313/2017–2017/2044(BUD))(4),
 - having regard to the Commission initiatives for the exploration of DLTs, among them ‘Blockchain4EU: Blockchain for Industrial Transformations’, ‘EU Blockchain and Observatory Forum’, ‘Blockchains for Social Good’ and ‘Study on the Opportunity and Feasibility of an EU Blockchain Infrastructure’;
 - having regard to Rules 128(5) and 123(2) of its Rules of Procedure,
- A. whereas Distributed Ledger Technology (DLT) and blockchain can constitute a tool that promotes the empowerment of citizens by giving them the opportunity to control their own data and decide what data to share in the ledger, as well as the capacity to choose who else can see them;
- B. whereas DLT is a general-purpose technology which can improve transaction cost efficiency by removing intermediaries and intermediation costs, as well as increasing transaction transparency, also reshaping value chains and improving organisational efficiency through trustworthy decentralisation;

- C. whereas DLT can introduce, through the necessary encryption and control mechanisms, an IT-based paradigm that can democratise data and improve trust and transparency, providing a secure and efficient route for the execution of transactions;
- D. whereas DLT promotes the pseudonymisation of users but not their anonymisation;
- E. whereas DLT is a still evolving technology which necessitates an innovation-friendly, enabling and encouraging framework that provides legal certainty and respects the principle of technology neutrality, while at the same time promoting consumer, investor and environmental protection, increasing the social value of the technology, reducing the digital divide and improving the digital skills of citizens;
- F. whereas DLT can provide a framework of transparency, reduce corruption, detect tax evasion, allow the tracking of unlawful payments, facilitate anti-money laundering policies, and detect misappropriation of assets;
- G. whereas DLT makes it possible to ensure the integrity of data, and the ability to provide a tamper-evident audit trail permits new models of public administration and helps bring about improved safety;
- H. whereas the regulatory approach toward DLT should be innovation-friendly and based on the principle of technology neutrality, enabling also the creation of innovation-friendly ecosystems and innovation hubs;
- I. whereas blockchain is only one of several types of DLTs; whereas some DLT solutions store all individual transactions in blocks which are attached to each other in chronological order in order to create a chain which ensures the security and integrity of the data;
- J. whereas cyberattacks are considered to have less impact on such chains, as they need to successfully target a large number of copies rather than a centralised version;
- K. whereas DLT can significantly improve key sectors of the economy as well as the quality of public services, providing high-level transactional experience to consumers and citizens and reducing the costs incurred by them;
- L. whereas questions and concerns related to the application of horizontal regulation and rules, on issues such as data protection or taxation, can inhibit the potential for development of DLT in the EU;
- M. whereas DLT applications have the potential quickly to become systemic, similarly to how digital innovations have fundamentally changed services in other sectors, such as telecommunications;
- N. whereas the risks and problems of the technology are not yet completely known;

DLT, decentralisation and applications

1. Stresses that DLT reduces intermediation costs in a trusted environment between the transacting parties and allows peer-to-peer exchange of value that can empower citizens, disrupt legacy models, improve services and reduce costs throughout value chains, in a wide range of key sectors;
2. Underlines the profound impact that DLT-based applications could have on the structure of public governance and the role of institutions, and asks the Commission to carry out a study assessing the potential scenarios of a wider uptake of public DLT-based networks;
3. Highlights the wide range of DLT-based applications that could potentially affect all sectors of the economy;

Energy- and environment-friendly applications

4. Underscores that DLT can transform and democratise the energy markets by allowing households to produce environment-friendly energy and exchange it on a peer-to-peer basis; stresses that such technologies provide scalability and flexibility for plant operators, suppliers and consumers;
5. Underlines that DLT can support the production and consumption of green energy and could improve the efficiency of energy exchanges; notes that DLT can transform the grid operation and allow communities and individuals to provide grid services as well as to integrate renewable resources more efficiently; also stresses that DLT can create alternatives to state-sponsored renewable investment schemes;
6. Notes that DLT can facilitate the energy transmission and distribution infrastructure and create a new transaction ecosystem surrounding electric vehicles; stresses that DLT improves energy reporting and enables accurate tracking of renewable or carbon certificates;
7. Stresses that DLT can support the electrification of poor rural communities through alternative payment and donation mechanisms;
8. Underlines the need to promote technical solutions that are less energy-consuming and are generally as environment-friendly as possible; stresses that several consensus mechanisms, among them 'proof-of-work', 'proof-of-stake', 'proof-of-authority' and 'proof-of-elapsed-time', have different energy consumption needs; calls on the Commission to add an energy efficiency dimension in its activities related to DLT and to explore through research initiatives the energy impact and energy efficiency of the various consensus mechanisms;
9. Calls for an assessment of governance models within the diverse consensus mechanisms under development, taking into account the potential needs of intermediary systems, actors and organisations in order to validate and verify the authenticity of the exchanges and to prevent fraudulent behaviour in good time;
10. Highlights that DLT can bring new opportunities to the circular economy by incentivising recycling and enabling real-time trust and reputation systems;

Appendix

Transport

11. Underscores the potential of DLT for mobility and logistics, including registration and administration of vehicles, verification of driving distances, smart insurance and charging of electric vehicles;

Healthcare sector

12. Highlights the potential of DLT to improve data efficiency and the reporting of clinical trials in the health sector, allowing digital data exchange across public and private institutions under the control of the citizens/patients;
13. Recognises the potential for improvement of the efficiency of the healthcare sector through electronic health data interoperability, identity verification and a better distribution of medication;
14. Notes that DLT allows citizens to control their health data and benefit from transparency thereon, and to choose which data to share, also with regard to their use by insurance companies and the wider healthcare ecosystem; stresses that DLT applications should protect the privacy of sensitive health data;
15. Calls on the Commission to explore DLT-based use-cases in the management of healthcare systems, and to identify benchmark cases and requirements that enable high- quality data entry and interoperability between different DLTs, depending on systems and on types of institution and their work processes;

Supply chains

16. Underlines the significance of DLT in improving supply chains; notes that DLT can facilitate the forwarding and monitoring of origin of goods and their ingredients or components, improving transparency, visibility and compliance checking, by providing assurances that sustainability and human rights protocols are respected in the place of origin of a product, thus reducing the risk of illegal goods entering the supply chain and ensuring consumer protection; notes that DLT can be used as a tool to improve the efficiency of customs officers for counterfeit checking

Education

17. Stresses the potential of DLT for verification of academic qualifications, encrypted educational certification (e.g. 'blockcerts') and credit transfer mechanisms;
18. Stresses that lack of knowledge about the potential of DLT discourages European citizens from using innovative solutions for their businesses;
19. Highlights the need to establish non-profit-making entities, for example research centres, that would be innovation hubs which would specialise in DLT technology in order to perform educational functions regarding the technology in Member State;

20. Calls on the Commission to explore the possibility of creating an EU-wide, highly scalable and interoperable network that makes use of the technological resources of educational institutions in the Union, with a view to adopting this technology for sharing data and information, thus contributing to the more effective recognition of academic and professional qualifications; also encourages Member States to adapt specialised curricula at university level in order to include the study of emerging technologies such as DLT;
21. Recognises that for DLT to be trusted, awareness and understanding of the technology need to be improved; calls on the Member States to address this through targeted training and education;

Creative industries and copyright

22. Underlines that for ‘digitalised’ creative content, DLT can enable the tracking and management of intellectual property and facilitate copyright and patent protection; emphasises that DLT can enable greater ownership and creative development by artists through an open public ledger that can also clearly identify ownership and copyright; highlights that DLT could help link creators to their work, thus enhancing safety and functionality in the context of a collaborative and open innovation ecosystem, especially in areas such as additive manufacturing and 3D printing;
23. Notes that DLT might benefit authors by bringing more transparency and traceability to the use of their creative content, as well as cutting down on intermediaries, with regard to them receiving payment for their creative content;

Financial sector

24. Highlights the significance of DLT in financial intermediation and its potential for improving transparency and reducing transaction costs and hidden costs by better managing data and streamlining processes; draws attention to the interoperability challenges that use of the technology can pose for the financial sector;
25. Welcomes the research and experimentation that major financial institutions have undertaken in the exploration of the capabilities of DLT; stresses that use of the technology can also affect financial industry infrastructures and disrupt financial intermediation;
26. Calls on the Commission and the financial authorities to monitor developing trends and use-cases in the financial sector;
27. Emphasises the volatility and uncertainty surrounding cryptocurrencies; notes that the feasibility of alternative methods of payment and transfer of value using cryptocurrencies can be examined further; calls on the Commission and the ECB to provide feedback on the sources of volatility of cryptocurrencies, identify dangers for the public, and explore the possibilities of incorporating cryptocurrencies in the European payment system;

DLT ecosystem

Self-sovereignty, identity and trust

28. Underscores that DLT enables users to identify themselves while being able to control what personal data they want to share; notes that a wide range of applications can allow different levels of transparency, raising the need for applications to be compliant with EU law; stresses also that data in a public ledger are pseudonymous and not anonymous;
29. Underscores that DLT supports the emergence of new models to change the current concept and architecture of digital identities; notes that as a result digital identity is extended to people, organisations and objects, and further simplifies identity processes such as ‘Know Your Customer’ while enabling personal control over data;
30. Stresses that personal data management implies that users have the capacity and the technical knowledge and skills to manage their own data; is concerned about the dangers of misusing one’s own data and vulnerability to fraudulent schemes due to lack of knowledge;
31. Emphasises that digital identities are imperative for the future of this technology; considers that Member States should exchange best practices on how to ensure the security of such data;
32. Underlines that although DLT promotes self-sovereign identity, the ‘right to be forgotten’ is not easily applicable in this technology;
33. Emphasises that it is of the utmost importance that DLT uses are compliant with the EU legislation on data protection, and notably the General Data Protection Regulation (GDPR); calls on the Commission and the European Data Protection Supervisor (EDPS) to provide further guidance on this point;
34. Stresses that trust in DLT is enabled by cryptographic algorithms that replace the third-party intermediary through a mechanism that performs the validation, safeguarding and preservation of transactions;
35. Stresses that trust in permissionless blockchains is enabled by cryptographic algorithms, the participants, the network design and the structure, and that third-party intermediaries can be replaced through a mechanism that performs the validation, safeguarding and preservation of transactions and accelerates the clearing and settlement of certain securities transactions; notes that the efficiency of the safeguards is dependent on the proper implementation of the technology, and that this calls for technological developments that ensure genuine safety, thus enhancing trust;

Smart contracts

36. Emphasises that smart contracts are an important element enabled by the DLT and can act as a key enabler of decentralised applications; stresses that the Commission needs to undertake an in-depth assessment of the potential and legal implications, e.g. risks relating to jurisdiction; believes that use-case monitoring will be beneficial in exploring the potential of smart contracts;

37. Emphasises that legal certainty surrounding the validity of a digital cryptographic signature is a critical step towards facilitating smart contracts;
38. Calls on the Commission to promote the development of technical standards with relevant international organisations such as ISO, ITU and CEN-CELENEC, and to conduct an in-depth analysis of the existing legal framework in individual Member States in relation to the enforceability of smart contracts; calls on the Commission, should potential barriers arise to the use of smart contracts within the Digital Single Market, to take appropriate measures to assess whether such barriers are proportionate; notes, however, that legal certainty can be enhanced by means of legal coordination or mutual recognition between Member States regarding smart contracts;

Interoperability, standardisation and scalability

39. Stresses that there is a constellation of DLT technologies with various technological characteristics as well as different mechanisms concerning governance (permissioned and permissionless distributed ledgers) and consensus;
40. Notes that ensuring efficiency requires interoperability: (i) between DLTs; (ii) between applications built on the same DLT; and (iii) between DLTs and legacy systems;
41. Welcomes the initiatives of organisations such as ISO to establish standards for DLTs; calls on the Commission to continue to collaborate with other international organisations in standards setting;
42. Emphasises the importance of taking a global approach to standards setting so that innovative companies are not regulated out of the EU;
43. Underlines that trust generation through DLTs requires extended numbers of robust and expanded distributed ledgers, in order to avoid the concentration of data in the hands of a few market players, since this might lead to collusion; encourages the creation of DLT hubs across the EU,

Infrastructure security

44. Recalls the importance of DLT infrastructure protection, and suggests that if we are to effectively reap the benefits of this technology, abuses of dominant position must not be allowed;
45. Calls on the Commission to closely monitor technological developments (such as quantum computing), assess technological risks, support resilience to a cyber-attack or a system breakdown, and promote data protection projects that ensure the sustainability of DLT platforms as part of the agenda of the EU Blockchain Observatory; calls on the Commission to allocate resources accordingly;
46. Encourages the competent authorities and the Commission to develop stress testing for DLT applications;

Strategic importance of DLT for public infrastructure

47. Underlines the efficiency potential of DLT for public sector services and management as regards reducing bureaucracy, especially with a view to enforcement of the eGovernment Action Plan, with particular reference to the EU-wide adoption of the digital Once-Only Principle (TOOP) and thus further reducing administrative burdens for citizens, businesses and public administrations;
48. Underscores the potential of DLT to decentralise governance and improve the capacity of citizens to hold governments accountable; calls on the Commission to explore the improvement of traditional public services, including inter alia the digitalisation and decentralisation of public registries, land registry, licensing, citizen certification (e.g. birth or marriage certificates) and migration management, in particular by the development of concrete use-cases and pilots; calls on the Commission also to explore DLT applications that improve processes related to the privacy and confidentiality of data exchanges, as well as access to e-government services using a decentralised digital identity;
49. Is aware of the risks associated with DLT applications, in particular the use of unpermissioned blockchain applications for criminal activities, including tax evasion, tax avoidance and money laundering, and insists that these issues must be monitored and addressed urgently by the Commission and the Member States; calls on the Commission, to this end, also to explore the potential of DLT in the areas of law enforcement, tracking of money laundering and shadow economy transactions, and tax monitoring;
50. Calls on the Commission to monitor the potential of DLT for improving the social good, and to assess the social impact of the technology;
51. Calls on the Commission to create DLT-based platforms that will allow the monitoring and tracking of EU funding to NGOs, thus increasing the visibility of the EU assistance programmes and the accountability of the recipients;
52. Stresses, bearing in mind the efficiency opportunities DLT brings, the potential of DLT European public sector blockchains, compliant with EU law, that will enable decentralised cross-border transactions between Member States, thus facilitating the development of more secure and streamlined services, regulatory reporting, and data transactions between citizens and the EU institutions;
53. Underlines that EU public sector blockchains would enable greater transparency, as well as more streamlined processing of information and development of more secure services for European citizens; stresses how a permissioned blockchain network shared between Member States could be designed in order to store citizens' data in a secure and flexible manner;
54. Calls on the Commission to evaluate the safety and efficiency of electronic voting systems, including those that employ DLTs, for both private and public sectors; encourages the further exploration of use-cases;

SMEs, technology transfer and financing

55. Welcomes the potential of DLT to improve existing value chains, transform business models and thus promote innovation-driven prosperity; highlights the impact of streamlining supply chains and increasing interoperability among firms;
56. Highlights that open blockchain protocols can lower entry barriers for SMEs and improve competition in digital marketplaces;
57. Stresses that SMEs can benefit from disintermediation by reducing transaction costs, intermediation costs and red tape; notes that the use of DLT requires investment in specialised infrastructure or high-capacity services;
58. Notes that innovative SMEs and start-ups need access to funding in order to develop DLT-based projects; calls on the EIB and the EIF to create funding opportunities that support DLT-based entrepreneurial endeavours to accelerate technology transfer;
59. Asks the Commission to partner with Member States in order to ensure legal certainty for investors, users and citizens, both active and passive, while encouraging harmonisation within the Union and studying the idea of introducing a European passport of DLT-based projects;
60. Underscores the potential of Initial Coin Offerings (ICOs) as an alternative investment instrument in funding SMEs and innovative start-ups and to accelerate technology transfer; stresses that lack of clarity with regard to the legal framework applicable to ICOs can negatively affect their potential; recalls that legal certainty can be instrumental in increasing investor and consumer protection and reducing the risks stemming from asymmetric information, fraudulent behaviour, illegal activities such as money laundering and tax evasion, and other risks as highlighted by the European Securities and Markets Authority (ESMA) in its 2017 report on ICOs; calls on the Commission to provide guidelines, standards and disclosure requirements, especially in the case of utility tokens that qualify more as a distinct asset class and less as a security;
61. Emphasises the dangers related to ICOs; calls on the Commission and the regulatory authorities concerned to identify criteria that enhance investor protection and articulate disclosure requirements and obligations for the initiators of ICOs; stresses that legal clarity is essential for unleashing the potential of ICOs and preventing fraud and negative market signals;
62. Underscores that ICOs can be an essential element within the capital markets union; calls on the Commission to explore the legal requirements that will allow this asset class to be blended with other financial vehicles in strengthening SMEs' funding and innovation projects;
63. Calls on the Commission to create an Observatory for the Monitoring of ICOs, as well as a database of their characteristics and taxonomy, distinguishing security and utility tokens; suggests that a model framework of regulatory sandboxes and a code of conduct accompanied by standards could be the beneficial outcome of such an observatory in terms of helping Member States explore ICOs' possibilities;

64. Welcomes the decision by the Commission and Council to include DLTs as a legitimate sector for funding in EFSI 2.0;

Policies for boosting DLTs in Europe

65. Stresses that any regulatory approach toward DLT should be innovation-friendly, should enable passporting, and should be guided by the principles of technology neutrality and business-model neutrality;
66. Urges the Commission and the Member States to develop and pursue digital skills training and retraining strategies that can ensure European society's active and inclusive participation in the paradigm shift;
67. Encourages the Commission and the national competent authorities to swiftly build up technical expertise and regulatory capacity, allowing for rapid legislative or regulatory action if and when appropriate;
68. Underlines that the Union should not regulate DLT per se, but should try to remove existing barriers to implementing blockchains; welcomes the Commission's approach of following a use-case method in exploring the regulatory environment around the use of DLT and the actors using it by sector, and calls on the Commission and the Member States to foster the convergence and harmonisation of regulatory approaches;
69. Calls on the Commission to assess and develop a European legal framework in order to solve any jurisdictional problems that may arise in the event of fraudulent or criminal cases of DLT exchange;
70. Notes that the use of cases is essential to the development of best practices in the DLT ecosystem and to the assessment and management of the effects on employment structure of automatising procedures;
71. Welcomes forward-looking research frameworks aimed at improving assessment of the potential opportunities and challenges of emerging technologies in support of better decision-making, and, concretely, welcomes the Commission's project 'Blockchain4EU: Blockchain for Industrial Transformations';
72. Asks the Commission and the Member States to develop common initiatives to raise awareness and train citizens, businesses and public administrations with a view to facilitating the comprehension and uptake of this technology;
73. Highlights the importance of research into and investment in DLT; notes that the post-2020 MFF should ensure funding for research initiatives and projects based on DLT, as basic research on DLT is needed, including on the potential risks and societal impact;
74. Calls on the Commission to raise awareness concerning DLTs, to undertake initiatives for the education of citizens regarding the technology, and to address the problem of the digital gap between Member States;

75. Recommends that existing and future DLT-related initiatives and pilot projects carried out by the Commission should be closely coordinated, possibly under the guidance of the EU Blockchain Observatory, so as to realise synergy effects and ensure the creation of real added value while avoiding costly double structures; invites the Commission to undertake regular exchanges with Parliament on the progress achieved in DLT-related pilot projects;
76. Asks the Commission to undertake policy initiatives that promote the competitive position of the EU in the field of DLT;
77. Emphasises that the Union has an excellent opportunity to become the global leader in the field of DLT and to be a credible actor in shaping its development and markets globally, in collaboration with our international partners;

◦
◦◦

78. Instructs its President to forward this resolution to the Commission and the Council.

Bibliography

- A report by the UK Government Chief Scientific Adviser. (2017). *Distributed Ledger Technology*. London: A report by the UK Government Chief Scientific Adviser.
- Adamski, D. (2009). Informatyzacja podmiotów realizujących zadania publiczne. W D. Szostek, *eAdministracja. Prawne zagadnienia informatyzacji administracji*. Wrocław.
- Anderson, R. (2001). *on: Security Engineering: A guide to Building Dependable Distributed Sy*. New York: Wiley.
- Anderson, R. (2008). *Security Engineering: A guide to Building Dependable Distributed Sy*. New York.
- Authority, E. S. (2017, November 17). Pobrano z lokalizacji https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_state-ment_firms.pdf.
- Baran, P. (1964). *On distributed communications: I. Introduction to distributed communications networks*. Santa Monica: the Rand Corporation.
- Barta, J. and Markiewicz, R. (1998). *Internet a Prawo*. Kraków.
- Barta, J. and Markiewicz, R. (2005). *Handel elektroniczny. Prawne problemy*. Kraków: Zakamycze.
- Bartorski, D. (2012). *Cyfrowa gospodarka. Kluczowe trendy rewolucji cyfrowej. Diagnoza, prognozy, strategie reakcji..* Warszawa : MGG Conferences sp. z.o.o.
- Beatge, D. (2002). W B. Kaminski, T. Henssler, H. Kolaschnik and A. Papatoma-Beatge, *Rechtshandlung eBusiness. Rechtliche Rahmenbedingungen fur Gaschefte im Internet* (p. 100 et seq.). Neuwied, Kriftel.
- Bhaskar, N. D. (2015). Bitcoin Mining Technology. W L. K. Cheun, *Handbook of Digital Currency* (p. 46 et seq.). New York.
- Bhaskar, N. D. and Kuo Chuen, D. L. (2015). Bitcoin Mining Technology. W D. L. Kuo Chuen, *Handbuch of Digital Currency*. Amsterdam, Boston, Helderberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokio: Elsevier.
- Biella, M. and Zinetti, V. (2016). <https://www.weusecoins.com/assets/pdf/library/UNICREDIT%20-%20Blockchain-Technology-and-Applications-from-a-Financial-Perspective.pdf>. UniCredit.
- Boucher, P., Nascimento, S. and Kritikos, M. (2017). *How Blockchain Technology could change our lives*. Bruksela.
- Burczyński, T. (2011). *Elektroniczna wymiana informacji w administracji publicznej*. Wrocław.
- Butkiewicz, E., Pietkiewicz, M., Prokurat, J., Rutkowski, P. and Wojdyło, K. (2014). *Wirtualne waluty*. Warszawa : Wardyński and Wspólnicy.

Bibliography

- Byrski, J. (2018). *Outsourcing w działalności dostawców usług płatniczych*. Warszawa: C.H. Beck.
- Cham, D. (1985, nr 10 (28)). Security without identification: transaction systems to make Big Brother obsolete. *Communications of the ACM*, p. 1030 et seq.
- COMMISSION, S. A. (2017, lipiec 25). *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*. Pobrano z lokalizacji <https://www.sec.gov/litigation/investreport/34-81207.pdf>
- Czachórski, Z. (1994). *Zobowiązania. Zarys wykładu*. Warszawa.
- Czarnecki, J. (2016). *Blockchain, inteligentne kontrakty i DAO*. Warszawa: Wardyński i Wspólnicy.
- Świerczyński, M. (2004). Jurysdykcja krajowa a prawo właściwe. W P. Podrecki, *Prawo Internetu* (p. 154–160). Warszawa.
- Świerczyński, M. and Żarnowiec, Ł. (2015). W M. Pazdan, *System Prawa Prywatnego. Tom 20b. Prawo prywatne międzynarodowe* (p. 840). Warszawa: C.H. Beck.
- Ducas, E. and Wilner, A. (2017, Nr. 72). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. *International Journal*, 538–562.
- Ehrlich, E. (1918). *Die juristische Logik*. Tubingen.
- Eodel, D. (1997, nr 46). Why Regulate Cybermoney. *The American University Law Review*, p. 1075 et seq.
- Fallenbock, M. (2001). *Internet und internationales Privatrecht*. Wien.
- M. Finck Blockchain Regulation and governance in Europe, University of Cambridge, UE 2019r.
- Flaga-Gieruszyńska, K., Gołaczyński, J. and Szostek, D. (2016). *Media elektroniczne. Współczesne problemy prawne*. Warszawa: C.H. Beck.
- Fridman, M. (1960). *A program of Monetary Stability*. New York.
- Fuchs, B. (2013). Lex mercatoria – pojęcie. W W. Popiołek, *System prawa handlowego. Tom 9, Międzynarodowe Prawo Handlowe* (p. 47–50). Warszawa: C.H. Beck.
- Furlog, J. (2012, November 5). *The evolution of the legal services market*. Pobrano z lokalizacji [http://www.law21.ca/2012/11/the-evolution-of-the-legal-services-mark-et-stage-1](http://www.law21.ca/2012/11/the-evolution-of-the-legal-services-market-stage-1).
- Garstka, M. and Piech, K. (2017). *Konsorcja i Rady Blockchain na Świecie*. Warszawa: Ministerstwo Cyfryzacji.
- Gautrais, V. (2016). <http://www.lex-electronica.org/articles/volume-21/lex-electronica-daujourdhui-a-demain/>
- Gołaczyński, J. (2004). *Umowy elektroniczne w prawie prywatnym międzynarodowym*. Warszawa: Wolters Kluwer.
- Goldenfine, J. and Leiter, A. (2018, May 19). *Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct*. Pobrano z lokalizacji https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3176363.

- Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G. and Xu, X. (2018, March 5). Pobrano z lokalizacji On legal contracts, imperative and declarative smart contracts, and blockchain systems: <https://doi.org/10.1007/s10506-018-9223-3>.
- Grzybczyk, K. (2015). W M. Pazdan, *System Prawa Prywatnego. Tom 20c Prawo prywatne międzynarodowe*. Warszawa 2015: C.H. Beck.
- Grzybowski, M. and Bentyń, S. (2018). *Kryptowaluty*. Poznań.
- Guido Governatori, F. I. (2018, Marzec 5). *On legal contracts, imperative and declarative smart contracts, and blockchain systems*. Pobrano z lokalizacji <https://www.springerprofessional.de/on-legal-contracts-imperative-and-declarative-smart-contract-s-an/15509768>.
- Haber, S. and Stornett, W. (1991, styczeń nr. 3). How to time-stamp a digital document. *Journal of Cryptology*, p. 99–111.
- Heun, S. (1994, nr 10). Die elektronische Willenserklärung. *CuR*, p. 595.
- Isay, H. (1929). *Rechtsnorm und Entchaidung*. Berlin.
- Jachowicz, M. and Kotulski, M. (2012). *Forma dokumentu elektronicznego w działalności administracji publicznej*. Warszawa.
- Johnson, D. and Post, D. (1996 nr. 48). *Law And Borders – the Rise of Law in Cyberspace*. Stanford Law Review.
- Johnson, D. and Post, D. (1996, nr. 48). Post Law And Borders – the Rise of Law in Cyberspace. *Stanford Law Review*.
- Jorgensen, S. (1968). *Vertrag und Recht*. Kopenhaga.
- Kant, E. (1971). *Uzasadnienie metafizyki moralności*. Warszawa.
- Kaufmann-Kohler, G. and Schultz, T. (2004). *Online Dispute Resolution: Challenges for Contemporary Justice*. Wolters Kluwer International.
- Kerikmae, T. and Rull, A. (2016). Theorising on Digital Legal (Outer)Space. W T. Kerikmae and A. Rull, *The Future of Law and eTechnologies* (p. 1–10). Cham, Heidelberg, New York, London: Springer.
- Khan, A. (2015/maj). Bitcoin – payment method or fraud prevention toll? *Computer Fraud & Security*, 18.
- Klam, C. (2002). *Die rechtliche Problematik von Glücksspielen im Internet*. Berlin.
- Klyta, W. (2002). *Spółki kapitałowe w prawie prywatnym międzynarodowym*. Kraków: Zakamycze.
- Knnapas, K. (2016). Legal Revolution or Evolution from the Perspective of de lege ferenda? W T. Kerikmae and A. Rull, *The Future of Law and eTechnologies*. Cham, Heidelberg, New York, London: Springer.
- Koch, F. (1998). *Internet-Recht. Praxishandbuch mit den neuen Medien – und Teledin-sterecht Checklisten und Musterverträgen*. München, Wien.
- Kolvart, M., Margus, P. and Addi, R. (2016). Smart Contracts. W T. Kerikmae and A. Rull, *The Future of Law and eTechnologies* (p. 134–136). Heidelberg, New York, London: Springer.
- Law, L., Sabett, S. and Solinas, J. (1997, nr 47). How to make cryptography of anonymous electronic cash. *The American University Law Review*, p. 1131 et seq.

- Lenz, K. F. (2014). *Japanese Bitcoin Law*.
- L. Lessig: Cod is law. On Liberty in Cyberspace, Harvard Magazine” <https://harvardmagazine.com/2000/01/code-is-law-html>.
- Lim, J. (2015). A Facilitative Model for Cryptocurrency Regulation in Singapore. W D. LEE Kuo Chuen, [w:] *Handbook of Digital Currency*.
- Machnikowski, P. (2015). Prawo zobowiązań w 2025 roku. Nowe technologie, nowe wyzwania. W A. Olejniczak, J. Haberko, A. Pyrżyńska and D. Sokołowska, *Współczesne problemy prawa zobowiązań* (p. 379–380). Warszawa.
- Machnikowski, P. (2016). W P. Gniewek, P. Machnikowski and E. Gniewek, *Kodeks cywilny. Komentarz*. Warszawa 2016: C.H. Beck.
- Maxwell, D., Speed, C. and Pschetz Larisa. (2017, nr 23(1)). Story Blocks: Reimagining narrative through the blockchain. *The International Journal Of Research into New Media Technologies*, p. 79–97.
- Maxwell, D., Speed, C. and Pschetz, L. (2017, nr 23). Reimagining narrative through the blockchain. *The International Journal of Research into New Media Technologies*, p. 79 et seq.
- Menthe, D. (1998, nr 69). Jurisdiction in Cyberspace: a Theory of International Spaces. *Michigan and Technology Law Review*, p. 69–103.
- Morabito, V. (2017). *Innovation Trough Blockchain*. Cham: Springer.
- Pak Nian, L. and LEE Kuo Chuen, D. (2015). A Light Touch of Regulation for Virtual Currencies. W D. LEE Kuo Chuen, *Handbook of Digital Currency* (p. 321–322).
- Papadopoulos, G. (2015). Blockchain and Digital Payments: An Institutional Analysis of Cryptocurrencies. W L. Chuen, *Handbook of Digital Currency* (p. 153–172).
- Patrick, G. and Bana, A. (2017). *Raport Rule of Law Versus Role of Code: A Blockchain-Driven Legal Word*. International Bar Association Legal Policy & Research Unit.
- Pazdan, J. (2009, Tom IV). Rozporządzenie Rzym II – nowe wspólnotowe unormowanie właściwości prawa dla zobowiązań pozaumownych. *Problemy Prawa Prywatnego Międzynarodowego*, p. 13–35.
- Pazdan, M. (2014). W M. Pazdan, *System Prawa Prywatnego, Tom 20a. Prawo prywatne międzynarodowe* (p. 557–558). Warszawa : C.H. Beck.
- Piech, K. (2017). *Podstawy korzystania z walut cyfrowych*. Warszawa.
- Piech, K. (2018, czerwiec 23). *Leksykon pojęć na temat technologii blockchain i kryptowalut*. Pobrano z lokalizacji https://www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_tehnologii_blockchain_i_kryptowalut.pdf/77392774-1180-79a-b-4dd5-089ffab37602.
- Polański, P. (2014). *Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego*. Warszawa: C.H. Beck.
- Popiołek, W. (. (2013). *System Prawa Handlowego, Tom 9, Międzynarodowe Prawo Handlowe*. Warszawa: C.H. Beck.
- Radwański, Z. (1977). *Teoria umów*. Warszawa.

- Railas, L. (2004). *The Rise of the Lex Electronica and the International Sale of Goods*. Helsinki.
- (2014). *Regulation of Bitcoin in Selected Jurisdictions*. Washington: The Law Library of Congress.
- Reinach, A. (1913). Die apriorischen Grundlagen de burgerliches Rehchts. W. *Jahrbuch fur Philosophie und phanomenologische Forschung Bd I tail II* (p. 685).
- Rogers, J., Jones-Fenleigh, H. and Sanitt, A. (2017). *Arbitrating Smart Contract Disputes*. <http://www.nortonrosefulbright.com/files/20170925-international-arbitration-report-issue-9-157156.pdf>.
- Roth, N. (2015, 44). An Architectural Assessment of Bitcoin. Using the System Modeling Language. *Procedia Computer Science* 44, p. 530.
- Roth, N. (2015 nr 44). An Architectural Assessment of Bitcoin. *Procedia Computer Science*, p. 527–536.
- Satosho, N. (2018, czerwiec 23). *Bitcoin: A Peer-to-Peer Electronic Cash System 2008*. Pobrano z lokalizacji <https://bitcoin.org/bitcoin.pdf>.
- Scherback, S. (2014, nr 7). How Should be Bitcoin Regulated. *European Journal of Legal Studies*, p. 45–91.
- Scherback, S. (2014, September 14). *Integrating Computer Science into Legal Discipline: The Rise of Legal Programming*. Pobrano z lokalizacji https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496094.
- Schultz, T. (2006). *Information technology and arbitration. A practitioner's guide*. Wolters Kluwer International.
- Sherborne, A. (2017, December). *Blockchain, smart contracts and lawyers*. Pobrano z lokalizacji https://www.google.com/url?sa=t&rcrt=j&q=&esrc=s&source=web&cd=1&ved=0ahUKewi_y9294qjcAhWMBiwKHa3gCUMQFggvMAA&url=https%3A%2F%2Fwww.ibanet.org%2FDocument%2FDefault.aspx%3FDocumentUID%3D17badeaa-072a-403b-b63c-8fbd985d198b&usg=AOvVaw1fDNjqMc9uJ2HdiIGS44eI.
- Sherborne, A. (brak daty). *Blockchain, smart contracts and lawyer*. Pobrano z lokalizacji https://www.google.com/url?sa=t&rcrt=j&q=&esrc=s&source=web&ccd=1&ved=0ahUKewi_y9294qjcAhWMBiwKHa3gCUMQFggvMAA&url=https%3A%2F%2Fwww.ibanet.org%2FDocument%2FDefault.aspx%3FDocumentUID%3D17badeaa-072a-403b-b63c-8fbd985d198b&usg=AOvVaw1fDNjqMc9uJ2HdiIGS44eI.
- Sójka, T. (2016). W G. Maciej, *Kodeks cywilny. Tom II. Komentarz*. Warszawa: C.H.Beck.
- Sussenberger, C. (47–49). *Das Rechtsgeschäft im Internet*. Frankfurt a.M, Berlin, Bern, Brussels, New York, Oxford, Wien.
- Szabo, N. (1997 Nr 9). Formalizing and Securing Relationships on Public Networks. *fi@st mand@y*, <http://ojphi.org/ojs/index.php/fm/article/view/548/469#>.
- Szostek, D. (2004). *Czynność prawna a środki komunikacji elektronicznej*. Kraków: Zakamycze.
- Szostek, D. (2012). *Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej*. Warszawa: C.H. Beck.

- Szostek, D. (2015). Quo vadis. Pięćdziesiąt lat kodeksu cywilnego. W P. Stec and M. Załucki, *90 lat kodeksu cywilnego. Perspektywy rekodyfikacji*.
- Szostek, D. (2018). Przechowywanie danych kancelarii w chmurze. W D. Szostek, *Bezpieczeństwo danych i IT w Kancelarii prawnej*. Warszawa: C.H. Beck.
- Szostek, D. and Świerczyński, M. (2007, zeszyt 2). Arbitraż elektroniczny. *Kwartalnik Prawa Prywatnego*, p. 471 et seq.
- Szostek, D. and Swierczyński, M. (2017). Wpływ nowych technologii na prawo prywatne międzynarodowe. W P. Kostański, P. Podrecki and T. Targosz, *Experientia docet. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Traple*. Warszawa: Wolters Kluwer.
- Szostek, D. r. (2018). *Bezpieczeństwo danych i IT w Kancelarii prawnej*. Warszawa: C.H. Beck.
- Szpor, G., Martysz, C. and Wojskyk, K. (2007). *Forma dokumentu elektronicznego w działalności administracji publicznej*. Warszawa.
- Szpyt, K. (2018). *Obrót dobrami wirtualnymi w grach komputerowych. Studium cywilnoprawne*. Warszawa.
- Trudel, P. (2001). La lex electronica. W C. A. Morand, *Le droit saisi par la mondialisation* (p. 221–268). Bruksela.
- Walport Mark (przedmowa). (2015). *Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser*. <http://fintechpoland.com/wp-content/uploads/2017/01/Technologie-rozproszonych-rejestrow-UK-GOFS-FTP-NASK-PL-1.pdf>. Pobrano z lokalizacji <http://fintechpoland.com/wp-content/uploads/2017/01/Technologie-rozproszonych-rejestrow-UK-GOFS-FTP-NASK-PL-1.pdf>.
- Weber, M. (1960). *Rechtssoziologie*. Neuwied.
- Wiebe, A. (2002). *Die elektronische Willenserklärung*. Tubingen.
- Wielens, K. (2016). *How Corporates Can Use Blockchain Technology Supply Chain Finance*. <http://www.thepaypers.com/expert-opinion/how-corporates-can-use-blockchain-technology-in-supply-chain-finance/763456>.
- Wiewiórowski, W. (2013). Prawne aspekty udostępniania usług administracji publicznej w modelu chmury. W G. Szpor, *Internet Cloud computing. Przetwarzanie w chmurach*. Warszawa.
- Wowerka, A. (2014). W M. Pazdan, *System Prawa Prywatnego. Tom 20a Prawo prywatne międzynarodowe* (p. 627 et seq). Warszawa : C.H. Beck.
- Zandberg-Malec, J. (2016). *Blockchain, inteligentne kontrakty i DAO*. Warszawa: Wardynski i Wspólnicy.
- Zimoch, D. (2016). Wpływ technologii blockchain na efektywność banku. *Studia ekonomiczne. Zeszyty naukowe* Nr 281.
- Zoll, F. (2004). *Klauzule dokumentowe. Prawo dokumentów dłużnych ze szczególnym uwzględnieniem prawa papierów wartościowych*. Warszawa: C.H. Beck.

The Author

Dr. Hab. Dariusz Szostek is a Professor of the Faculty of Law and Administration at the University of Opole, Head of the Centre for Legal Problems and New Technologies at the University of Opole, Partner and founder of the law firm Szostek-Bar and Partners. Member of the Polish Academy of Sciences in Katowice, expert in new technologies, co-author of the e-court concept, originator of the electronic confirmation of receipt (electronic stanza currently introduced in MS), author of the concept of the electronic administration office and changes in the code of civil procedure, parliamentary expert, lecturer, author of several dozen publications (including monographs and foreign publications including bestsellers, among others, co-author of *Cyber Law* - issue in New York, Tokyo, Sydney, Amsterdam, London).

