Chapter III. Blockchains in finance[93]

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 1980s[94] (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 finance[95]. These were innovative solutions[96] (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 money[97], including whether it should function in transactions anonymously[98], (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, Wardyński 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 Nakamoto[99], 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 experts[100]. 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 framework[101]" (Friedman, 1960).

Blockchains in financial institutions

In 2012, the European Central Bank published its first report on virtual-currency schemes[102] 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 report[103] 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 sector[104]. 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 established[105] 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 (Citicoin) and UniCredit is analyzing blockchain-based payments[107] (Biella and Zinetti, 2016).

In Germany[108], 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.

larisBank[109], 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, Deutche 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 Peru[111].

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.

Bitcoin[112] and its Bitcoin blockchain

For the first time, a blockchain was used in practice to create the Bitcoin cryptocurrency, as an element of Bitcoin software[113]. 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-tym-ing-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 blockchchain).

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 bitcoins[115]. 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 number[116]. 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 Srebny.

may check what transactions[117] 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 wallet[118]. 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 blocks[120]. 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 consensus[121] in case of need[122]. 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 transactions[123], 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 2140[125] (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 block[126].

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 protocol[127]. It is very easy to verify it, while generating it requires a gigantic number of attempts[128].

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 cryptocurrencies[129]. (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 code[131]. 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 BSDL (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 threats[134] – 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 law[135], 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 vacuum[137] (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] Experienta 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. Machnikowski[138] (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 law[139]. 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 territorialism[140]. (Grzybczyk, 2015). The author indicates that the request for protection against violations of the copyright to online works[141] 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 online[142].

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 the 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 systems[145]" (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 citizen[146].

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"[149][150] (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 criteria[151] 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, character[153]. 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 number[154]. 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 clause[155], 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 Schnitzer[156], 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 obligations[158], 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 internę et en droit international prive, 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 contract[159] (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 law[160].

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 EU[161]. 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 standards[163]" (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 law[164].

> "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. Swierczyński: Jurysdykcja krajowa a prawo właściwe [in:] Prawo Internetu, ed. P. Podrecki, Warsaw 2004 pp. 154-159 (cited as "Jurysdykcja, 2004").

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

164 M. Swierczyński; Jurysdykcja, 2004, p. 156.

165 M. Swierczyński: Jurysdykcja, 2004, p. 156.

in referring to the law of the country of origin in the fields coordinated by the directive[166].

> "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 law[167]".

Both M. Fallenbock[168] and M. Świerczyński[169] 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 Justice[170] 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 Wettbewersrecht, Jus Privatum Bd. 54 2000rr, p. 57.
167 M. Swierczyński: Jurysdykcja , 2004, p. 157.
168 M. Fallenbock: Internet und internationales Privatrecht, pp. 203-204.
169 M. Swierczyński: 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 provided[171] (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 exact[172]), 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 methods[173]. 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 include[174]: 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 license[175] (it is an MIT license[176]). 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 copies[177] 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 Electrum[178], 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 signing[179]. 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 software[180] 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 wallet[182].

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 obligations[185], 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 classification[186]" (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, Ł. Zarnowiec, 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 world[188]. 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 Bank[189], 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 security[190] (Pak Nian and LEE Kuo Chuen, 2015).

"Cryptocurrency-exchange" regulations were also introduced[191] in other states, such as Singapore[192] (Lim, 2015), Japan, Switzerland and Belarus, where Decree No. 8 of the President of Belarus introduced the regulation regarding development of the digital economy[193]. 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.legislature.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&l=1, access on 8 November 2018.
195 http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&l=1, access on 8 November 2018.
196 http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=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 protection[197]. 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 technologies[199] (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 ATMs[200]. 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 regulations[201]" (Papadopulos, 2015).

201 G. Papodopoulos: 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 money[202] 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/virtualcurrencyschemesen.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 209/110/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.