Chapter II. Blockchains, DLT – basic terms.

It would be impossible to attempt to discuss the legal issues of using DLT and blockchains without first defining a number of technological terms used in this study, as well as in the publications, discussions and reports connected with the digital economy. The difficulty is connected to the technical character of these terms and to a lack of uniform legal definitions due to their innovative character. Many remarks regarding DLT or blockchains result from a wrong understanding of those terms or from different points of view, depending on the profession of the speaker. The purpose of the following proposed definitions is to present the issues to lawyers and to present the conceptual framework used in this monograph, as well as to indicate how that issue was solved in the statutory laws of certain states[38].

DLT – distributed ledgers

Definition

Development of informatization may be divided into several stages. At the beginning (when computers were gigantic, but with very poor computing power in comparison to contemporary mobile devices), calculations and other data were stored locally, on one computer[39]. Additionally, at that time it was impossible to transfer data (apart from physical transfers of the punched tapes used for programming the first computers). Development of information technology was dependent on the development of commu-

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

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

nication[40]. The possibility to connect two and more computers allowed a significant improvement of their computing power. The so-called "Metcalfe's law" states that the usefulness of computer networks is proportional to the square of the number of its connected nodes. In turn, a *computer network node* (a so-called *node* – a term significant for blockchains) is an active electronic device connected to the network which allows the sending, receiving and transfer of information through a channel of communication[41]. In 1964 Paul Baran, in his memorandum[42] RM-3420-PR "On distributed communications: I. Introduction to distributed communications networks" (Baran, 1964) published the breakthrough concept (in just 37 pages) of information distribution.[43]

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

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

A *distributed network* does not have a central server, and transfers data using the shortest route possible[44].

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

---

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

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

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

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

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

The term "DLT" (distributed ledger technology), was introduced in "A report by the UK Government Chief Scientific Adviser" in 2015[45] (publication in January 2016).

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

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

Legal definition

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

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

---

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

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

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

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

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

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

In July 2018 (5th July), the Maltese lawmakers adopted a set of acts regarding blockchains. In the Malta Digital Innovation Authority Act C901[50], it defined "DLT", "distributed ledger technology", in the following manner: "'decentralised ledger technology' means a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes, or any variations thereof, as further described in the First Schedule of the Innovative Technology Arrangements and Services Act, 2018, and the term "node" means a device and data point on a computer network"; under which software and architectures which are used in designing and delivering DLT which ordinarily, but not necessarily: a) uses a distributed, decentralized, shared replicated and ledger, b) may be public or private or hybrids thereof; c) is permissioned or permissionless or hybrids thereof; d) is immutable; e) is protected with cryptography; and f) is auditable.

DLT and documents

The DLT (distributed ledger) technology is closely connected to the latest concepts of understanding the term "document", under which authorized information is more important than the formal document containing it, so-called "access to information in place of document[51]" (Szostek D., Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej, 2012). The essence of a document may be seen in the recording of information in a relatively permanent manner, so that it is possible to disclose it, reproduce it, copy it or transfer it to another medium in an unchanged condition. In the doctrine, but also in the judicature, there are listed several basic elements of a document: 1. medium 2. information 3. recorded so as to allow someone

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

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

to get to know its content[52]. For hundreds of years, documents were recorded in a tangible form (clay tablets, parchment, paper, etc.), with a kind of physical unity of the (tangible) medium and the information recorded thereon. Digitization, and the resulting paperless format, is consistently leading to a change in one of the elements of a document, i.e., its medium[53]. It is worth noting that since 1 July 2016, under art. 3 point 35 of the eIDAS regulation, applicable directly to all the legal orders of the EU countries, an electronic document is any content stored in electronic form, in particular a text or a sound, video or audiovisual recording. The term 'medium' is neutral and not necessarily connected to its traditional, physical meaning, which is visible in the recent evolution of that term[54], including recording in clouds, or in a distributed manner.

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

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

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

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

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

phone, tablet, etc.) as the access device that does not store data or documents[55]. That system continues to be a centralized one.

In time, there appeared the concept of sharing documents and of interactivity which resulted from, among others, a different approach to documents and to the manner in which they are stored, i.e., not as a complete thing but as data that may be accessed using the proper software[56].

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

Information verification takes place automatically through IT systems based on cryptography and data-transfer protection[57]. That information is approved after verification by the persons (or nodes – devices) authorized to it, e.g., the node of the given state, local authority, etc. It is possible (although impractical) to introduce the mechanism of acceptance by specific natural persons.

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

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

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

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

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

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

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

Blockchains

Definition

The term 'blockchain', earlier 'block chain', is already 10 years old. It was first used by a group of IT specialists/enthusiasts but, with the growing popularity of Bitcoin and other cryptocurrencies, has become successively more and more commonly used, becoming one of the most popular terms used in 2018. The concept of the origin of blockchain technology dates back to 2008 and to the publication of a white paper on cryptography by the person or persons operating under the nickname Satoshi Nakamoto[59] (Satosho, 2018) (Ducas and Wilner, The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada, 2017). The document proposed the introduction of an electronic version of money, allowing direct peer-to-peer (P2P) payments so as to eliminate participation in the payment system of central authorities and intermediaries. That technology was to (and currently is) based on blockchain technology. However, the very concept of using cryptography dates back practically to the beginning of computerization. In turn, the idea for a cryptographically secured chain of transaction blocks was described by Stuart

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

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

Haber and W. Scott Stornett in 1991[60] (Haber and Stornett, 1991) and developed by R. Andreson[61] (Anderson, Security Engineering: A guide to Building Dependable Distributed Sy, 2008) (Anderson, on: Security Engineering: A guide to Building Dependable Distributed Sy, 2001).

A report for the British government[62] (Walport Mark (przedmowa), 2015) indicated that a blockchain is a type of database that takes a number of records and puts them in a block (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows blockchains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions.

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

In another report, Deloitte Australia[63] indicates that a blockchain is to be understood as a distributed book used for recording and sharing information in peer-to-peer networks. Identical copies of a ledger are maintained and jointly verified by network members, and the accepted information is aggregated in "blocks" that are added in a chronological "chain" of existing and approved blocks, using cryptographic signatures. Each new block has a time stamp corresponding to the development of new and permanent data – it contains the information on the preceding block, ensuring that each attempt to change it would require the changing of each of the blocks saved earlier[64]. The authors of that definition indicate that that technology is extraordinary due to the possibility to ensure digital authenticity using cryptographic "evidence". It is transparent and allows fast and cheap transmission of information and values in vast networks.

---

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

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

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

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

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

Two elements typical for blockchains were indicated by D. Maxwell, Ch. Speed, L. Pschetz[65] (Maxwell, Speed and Pschetz Larisa, 2017) : the first one is that it provides a response to the "missing link" of the digital system (allowing the introduction of "counterparts" of uncopiable digital goods that are verified and tracked in a network book (ledger)), and the second – that it is an undertaking characterized by (joint) participation.

Legal definition

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

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

The very innovative element is considering a signature secured by blockchain technology to be a signature meeting the requirements of an electronic form, and considering a document or contract secured by blockchain technology to be a document or contract in electronic form[67]. Art. 5 allows smart contracts to be used in business dealings. Therefore, it will be impossible to dismiss the effects of a contract solely for the reason that it has been concluded as a smart contract. Furthermore, regardless of other regulations, it is considered that the data secured using blockchain technology is equivalent to other data, secured in other ways. That principle applies to ownership-transfer contracts or contracts for use.

---

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

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

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

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

missed[68]. On 30 May 2018, the S. 269 Act Related to Blockchain Business Development was adopted, in which the blockchain definition included in 12 V.S.A. was repeated and the following additional definition was introduced: ""Blockchain technology" means computer software or hardware or collections of computer software or hardware, or both, that utilize or enable a blockchain.

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

On 21 December 2017, the President of Belarus issued decree No. 8 on the development of the digital economy (effective from 1 January 2018). The decree specifies the general principles of functioning of the digital economy in Belarus and opens the economy to foreign technologies, including IT specialists (among other details, they do need a visa or a work permit). The operations of cryptocurrency exchanges and trading in tokens were formally allowed, and appendix No. 2 to the decree introduced new terms, including the following definition: Transaction block ledger (blockchain) – a sequence of blocks with information about operations performed in such a system built on the basis of given algorithms in a distributed decentralized information system using cryptographic methods of information protection[70]. An interesting addition, unseen in other states, was the introduction, in legal regulations, of the definition of (mining) related to blockchains. The regulation introduced and functioning from 1 January 2018 is very modern and meets the needs of participants in the digital economy (including, for the purpose of settlements, that an operator

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

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

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

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

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

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

Blocks

Blockchain technology uses so-called blocks, differently from classical DLT, which is a component of blockchain technology[72] (Maxwell, Speed and Pschetz, Reimagining narrative through the blockchain, 2017). It consists of a heading and data (transactions).

The heading contains a reference to the preceding block in the chain (the so-called hash), then a time stamp that specifically indicates the time of establishment and the so-called merkle tree root of all transactions included in the block[73] (Roth, 2015).

The same data block contains 1) the merkle tree root of all the transactions included in the block and 2) the transactions of the given block[74] (Piech, 2018).

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

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

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

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

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

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

Hash is a short combination of characters assigned to a dataset of any size using a hash function. In blockchain technology, it is important that it is resistant to double generation of the same hash to different datasets and that it is unidirectional, i.e., that it is impossible to obtain the data based on the hash value itself[75]. The hash function has been successfully used for many years in PKI in the scope of qualified electronic signatures, time stamps and qualified electronic stamps, wherever it is required to guarantee authenticity and integrity of signed data and, as a result, its confidentiality and non-repudiation.

A blockchain contains the full history of a transaction, available to everyone and stored by everyone. The transaction is grouped in blocks. The number of transactions depends on the size of the data. The limit for a block may be different, e.g., in Bitcoin it is 1,000,000 bytes. The heading consists of seven fields, while the block version number depends on the version of the software used for generating it. The SHA256 hash of a heading must be lower than or equal to the calculated current hash (the so-called mathematical problem to be calculated by the miners) for the block to be accepted. The number of transactions included in the block is displayed in the heading field[76] (Bhaskar and Kuo Chuen, 2015).

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

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

Consensus

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

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

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

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

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

PoW as an algorithm "looks after" the reaching of a *consensus*, or "the process within which the parties taking part in a network based on blockchain technology agree to conduct a transaction approved by all the participants in the network[78]" or by the entities authorized to approve it (e.g., ledger operators). PoW is an algorithm used for acceptance of and approval for Bitcoin blockchains, among others.

Other ways of reaching consensus indicated in the literature[79] (Piech K. , 2017) include:

Proof-of-Stake (PoS) a "method based on the amount of currency possessed. The more units of the given currency a participant has, the bigger the chance that it will establish a block[80]". A little broader definition was indicated by V. Morabito (Morabito, 2017) – he stated that PoS is an alternative to PoW, and proof and consensus do not require such costly calculations as PoW. PoS depends on the participation by entities within the given holding. A block is confirmed and established by whoever has a greater share[81].

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

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

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

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

78 K. Piech, Leksykon, 2018, p. 8.
79 K. Piech (ed.) Podstawy korzystania z walut cyfrowych, Warsaw 2017, p. 22.
80 K. Piech (ed.) Podstawy p. 22.
81 V. Morabito: Business Innovation Through Blockchain, Cham (Springer) 2017, p. 11.
82 K. Piech (ed.) Podstawy, 2017, p. 22.
83 V. Morabito: Business Innovation Trough Blockchain, p. 12.

How does it work?

In order to explain the principle of blockchain technology, we should examine the traditional ways of maintaining ledgers. Since the dawn of time, business dealings, in particular circulation of goods, values, etc., have been based on recording of facts (sometimes whole documents) for evidentiary purposes, in particular for demonstrating the rights entered in the ledger. Ledgers are maintained by the so-called trusted entities – established, functioning and controlled in accordance with proper legal regulations (e.g., banks maintaining the accounts, courts maintaining the trade registers, land and mortgage registers, etc., accountants keeping accounting books). These registers, as indicated before in discussion of DLT, are usually centralized, and in trading there appears an intermediary trusted by all the users, with full control over the system, who assists in transactions[84]. In practice, the users (e.g., bank clients) do not directly control the entries (in the system), but may only exercise follow-up control and raise claims in the case of violation of laws or occurrence of liability for damages. The data and base are centralized (having nothing more than backups). However, apart from access to that base, a user does not have a "copy" thereof. This means that, in practice, in the case of a banking-system failure, the persons holding bank accounts may not prove their rights or the fact of performing, for example, a banking act, or it is highly difficult.

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

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

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

to record a transaction, what might be necessary is acceptance by the seller (confirming, among others, its account and the fact that it is transferring the ownership of a thing) and by the buyer (that it purchases that thing and pays for it (today, in practice, when transferring money, the beneficiary does not have to consent to anything, and there are frequent mistakes in account numbers)). The process of verification and consent is performed fully automatically (today, when using electronic banking, everything is fully automatic on the part of the bank). Transactions are performed by many users of the system at the same time, and these transactions (after approval, naturally) are joined and registered in blocks and cryptographically secured by the so-called miners (as there are many transactions, they wait for "their turn" to become joined in a block). If someone is in a hurry, they may "purchase" priority of entering the given transaction in a block, by declaring the amount of commission to be obtained by the miners at the given transaction. In order to imagine that process, we may compare the respective blocks to a sheet of paper, on which many participants enter their transactions (e.g., declarations by the seller and buyer), everyone enters their transaction and signs it, thus authorizing the previous transactions on the sheet, until there is no more space. Then, a list of contents is generated with a reference of where the given declaration is (i.e., a heading and hash tree root are generated). When the sheet is complete, it is secured (e.g., with a stamp) and another one is started which, after being filled in, is attached to the previous sheet (e.g., glued together) and joined to it, e.g., with a signature and impression of a stamp on the borderline between the sheets. An identical activity takes place in a blockchain, by adding a link to a chain of transactions and securing it. The chain makes up the ledger, to which all the users are entitled[85] (Khan, 2015/maj) (and have a "copy" thereof saved on their devices, or rather an identical, integral and cohesive part of the ledger). Such activity is called mining. Additionally, on the network computers (so-called diggers), there is simultaneously being solved a complicated mathematical problem consisting of generating a properly encrypted block of transactions (proof of work) which is added to the blockchain (thus guaranteeing cryptographic security). It is as if, on a traditional sheet, the best artists prepared a complicated drawing, the best of which (and consistent with the problem visible on the sheet) is placed on

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

it as additional security, so that the sheet may not be forged[86]. Adding another block to the chain means updating the lodger of all the users, including previous ones. Acceptance of a block takes place only when the transactions included therein are verified. If there are discrepancies, the block is rejected. The chain generated in that manner is very difficult to alter, and currently practically impossible taking into account the large computing power of the participating computers. It would also be very difficult, or even impossible, to destroy it, because there are as many "copies", or actually identical ledgers, as there are users, and destroying a ledger would require a simultaneous and effective attack on all the "counterparts". Also, it is impossible to have a "false register", because every user has their own, true version which may be compared with others[87]. Just like before the era of digitization, "home" documents could be compared with others, e.g., from a bank (although at that time it was not one distributed ledger, but rather distributed documents).

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

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

---

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

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

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

Types of blockchains

Blockchain technology may be applied in different ways. There are three basic types of blockchains: public, private and hybrid[89]. The best-known and revolutionary one is a public blockchain, mainly for the reason that it is the foundation for Bitcoin. A public blockchain is fully open-source, within which everyone, without any personal or territorial limitation, may install suitable software their own device and download the whole or any fragment of a database and, usually (like in the case of Bitcoin), make its "copy" available to other nodes. Operations within private blockchains usually do not require the consent of the ledger operators. What is needed is consensus from the users. Public ledgers, such as Bitcoin, do not have one "owner" and are resistant to censorship, which means no one can block the entering of a transaction in the ledger[90].

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

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

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

89 V. Morabito: Business Innovation Through Blockchain, p. 8.
90 http://fintechpoland.com/wp-content/uploads/2017/01/Technologie-rozproszonych-rejestrow-UK-GOfS-FTP-NASK-PL-1.pdf p. 13.
91 K. Piech: Leksykon, 2018, p. 6.

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

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

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

92 Classification presented by K. Piech: Leksykon.