The Opinion of the Hungarian National Authority for Data Protection and Freedom of Information on Blockchain Technology in the Context of Data Protection

A Hungarian citizen requested the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter the Authority) to deliver its opinion on the data protection issues of the use of the virtual currency bitcoin and the blockchain technology underlying it. Having a general nature and touching a novel technology of public interest, the Authority publishes its opinion on the technology on its website.

1) The Definition of Personal Data, the Legal Basis of Data Processing, the Concepts of Data Controller and Data Processor

Section 3 (2) of Act CXII of 2011 on the Right of Informational Self-determination and on Freedom of Information (hereinafter the Privacy Act) defines the concept of personal data. This legal definition[1] extends legal protection to all data (e.g. name, identification mark, physical, mental, economic, and social features) that can be associated with the natural person concerned, the data subject, as well as the consequences that can be drawn from them.

Section 5 (1) a) and b) of the Privacy Act stipulates that the possible legal basis of processing personal data may be *the prior consent of the data subject* or *a provision of law for the purposes of public interest.*[2] When data processing is required by law, it is to be deemed mandatory, and is not conditional on consent by the data subject. Section 6 (1) of the Privacy Act, however, establishes a further legal basis for the processing of personal data, as it states that personal data may be processed also if it is necessary for *compliance with a legal obligation* pertaining to the data controller or *for the purposes of the legitimate interests* pursued by the data controller or by a third party when obtaining the data subject's consent is impossible or it would give rise to disproportionate costs and enforcing these interests is proportionate to the limitation of the right for the protection of personal data.[3]

---

[1] Section 3 (2) of the Privacy Act states: '"personal data" shall mean data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject'.

[2] According to Section 5 (2) a)–b): personal data may be processed when the data subject has given his prior consent, or when processing is rendered necessary for purposes of public interest by law or local government decree empowered by law for a predefined range (hereinafter mandatory data processing).

[3] According to Section 6 (1) a)–b) of the Privacy Act: personal data may be processed also if obtaining the data subject's consent is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary for compliance with a legal obligation pertaining to the data controller, or for the purposes of the legitimate interests pursued by the controller or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data.

If the data subject's prior consent, a legal basis provided for by law, and a verifiable, proportionate and legitimate interest are unavailable, the data controller is not entitled to process personal data.

Section 3 (9) of the Privacy Act defines the concept of data controller, stating it is any natural or legal person, or organisation without legal personality which alone or jointly with others determines the purposes and means of the processing of data; makes and executes decisions concerning data processing (including the means used) or have it executed by a data processor.

Section 3 (10) of the Privacy Act means by data processing any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans).

The data controller is not to be confused with the data processor, who Section 3 (18) of the Privacy Act defines as any natural or legal person or organization without legal personality processing the data on the grounds of a contract, including contracts concluded pursuant to legislative provisions. Data process is defined by Section 3 (17) of the Privacy Act as the performing of technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data.

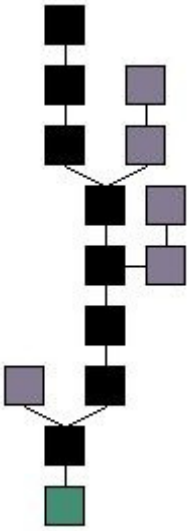
2) Outline of the Technical Background of the Blockchain Technology

The first representative of the blockchain technology was the virtual currency bitcoin on the digital market. This currency exists only virtually, and therefore has no physical embodiment, the consumer cannot encounter it in the form of coins or banknotes. The bitcoin has no central issuer, it is not printed in the way money in the physical sense is; it comes into being as a result of virtual 'mining'. It is the computers of the individual users that do the mining, and thereby produce newer and newer coins.[4] In what follows, we shall present the behaviour of data processed in a blockchain through the technology underlying the bitcoin, the most widespread blockchain-based system.

In a blockchain, data are stored in so-called blocks, which practically function as small databases. If new data are added to the decentralized database of the blockchain by the

[4]Joshua Davis: 'The Crypto-Currency – Bitcoin and its Mysterious Inventor', *The New Yorker,*10 October 2011, http://www.newyorker.com/reporting/2011/10/10/111010fa_fact_davis

users, they will be stored in a new block. In the course of making blocks, a chain is created, hence the name 'blockchain'. A blockchain is valid if it is headed by a so-called 'genesis block' (the first block made), and if all the transactions made with the data in them are valid. There is only a single, straight way back to the genesis block, as shown by the following illustration.



The system stores not only the data in the block but also all the operations made with them within the system. Data transactions are carried out without actual data movement between blocks; instead, the system merely attributes to the individual data in the block it is stored in the user entitled to dispose with it. The system adds the digital signatures of the users to the data stored in the blocks, and it is on this basis that it determines which user is entitled to dispose with the dataset in the given block.

In the bitcoin system, 'ownership right' over the respective coins is attributed to the given user by, for example, the user 'signing' with his or her digital signature every transfer of the virtual coins (this is the so-called 'public key' and 'private key' pair. The data stored in the bitcoin blocks are the coins, and the right of ownership over them is actually a chain of digital signatures.[5]

The basis of the blockchain-technology storage is a decentralized system in which there is no central entity or any other external organ that controls the transactions made with data in it. The blockchain is stored not by a central data controller but by practically all users on each of their computers.[6]

In, for example, the bitcoin system, which is based on blockchain technology, this type of decentralized storage operates in such a way that the bitcoin client software running on

[5]Satoshi Nakamoto: 'A Bitcoin matematikai alapjai', http://bitcoin.hu/?page_id=316
[6]Gerald P. Dwyer: *The Economics of Bitcoin and Other Private Digital Currencies*. University of Carlos III, Madrid, ECO-2010-17158 Project, 2014. p. 2.

each user's computer downloads every single 'bitcoin block' on to its hard disk, and thereafter all new ones. The full database of the transactions of the data stored in the blockchain are thus on each computer of the bitcoin users, and is continually updated through the open network. For a transaction to be performed, at least six other computers in the network must verify it.[7]

3) Who Qualifies as a Data Controller and a Data Processor with Regard to Blockchain? What is the Legal Basis of Data Processing?

The blockchain technology underlying the bitcoin system was developed to enable a virtual currency system to be used anonymously, as there would be no need of providing personal data for carrying out bitcoin operations. Nevertheless, it is possible to conceive of a system using blockchain technology where blocks store personal data, as well; thus, for example, personal data could be linked to the data stored in a block and used fundamentally for payment.

If the blocks in a chain are used also for storing personal data, the question arises who qualifies as the data controller. In accordance with the concepts of the Privacy Act outlined above, the data controller is primarily the legal or natural person that determines the purposes of processing data, makes and executes decisions concerning it. Due to the fact that the blockchain is a decentralized system where there is no central entity exercising supervisory rights over system operations and data transactions, it is the individual users that practically carry out the data processing.

With regard to the blockchain, thus, each user who adds blocks and data within them to the system (e.g. one who 'mines' in the bitcoin system) simultaneously qualifies as a data controller, as well. Over time, the user who adds data to the system will receive the exclusive right of disposal over his or her data stored in the block, and can therefore determine which transactions he or she wants to use the data for.If the right of disposal over the personal data in a block is transferred to another user, thenceforth this user (the addressee of the data) obtains exclusive rights over the data, and thus qualifies as the data controller.

In respect of the blockchain technology, the concept of data processor applies if the original data controller entitled to dispose of the data engages another user to carry out predefined data processing operations (e.g. transactions) by way of, for example, a contract of agency.

Under effective law, the legal basis of processing personal data stored in the blockchain is the consent of the data subject or the legitimate interest of the user (Sections 5 (1) a) and 6 (1) of the Privacy Act). Should the data subject not consent to the storing of or carrying out

[7] https://en.bitcoin.it/wiki/Blocks

operations with his or her personal data by the user entitled to dispose of data stored in the block, or should the user not be able to prove a legitimate interest in data processing, then data processing is unlawful.

4) The Problem of Jurisdiction Regards the Use of Blockchain Technology

As mentioned above, all users that carry out operations with the data for their own purposes qualify as data controllers also as a result of the decentralized nature of the blockchain technology. Due to this decentralized feature, the data controllers may carry out their data processing activities even under the jurisdictions of several different states.

Established on the basis of Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the Directive),the Article 29 Data Protection Working Party set forth the following in its opinion no. 1/2010 on the concepts of 'data controller' and 'data processor': 'being a data controller is primarily the consequence of the factual circumstance that a legal entity has chosen to process personal data for its own purposes'.[8]

Furthermore, the Working Party explained that the definition of the concept of the data controller has a prominent role in determining which state's national law applies to the given data processing or the individual operations done on the data. According to Article 4 (1) a) of the Directive, the main rule is that each Member State must apply its own national provisions when the data processing '*is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*'.

According to Opinion 8/2010 (WP179)[9] on applicable law of the Working Party, it is the notion of the '*context of activities*' of the establishment, not the place of storing personal data, that is decisive for determining applicable law. This notion means not that the applicable law is the law of the Member State where the data controller resides, but where an organ of the data controller participates in the activities related to the data processing. If an entity processes personal data in the framework of its own activities, the applicable law is the law of the Member State where it resides.

With regard to the above, the Authority calls attention also to the fact that the Court of Justice of the European Union (hereinafter the ECJ) in its judgment of 1 October in case 2015 C-230/14 interpreted the concept of settlement even more broadly than in its judgment of 13 May 2014 in case C-131/12 (the so-called Google Spain ruling). In judgment C-230/14, the ECJ ruled that Article 4 (1) a) of the Directive must be interpreted so as to permit the

[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf#h2-2
[9] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf#h2-2

application of the law on the protection of personal data of a Member State other than the Member State in which the data controller with respect to the processing of those data is registered, in so far as that data controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity—even a minimal one—in the context of which that processing is carried out.

The question of jurisdiction is therefore determined by the clarification of the preliminary question of on the territory of which state the data controller defining the purpose of data processing carries out the processing of data. In terms of the blockchain technology, this means that the state will be the one where the data controller carries out the activities related to data processing, thus e.g. commands a transaction, accesses a blockchain, and adds data to it—e.g. 'mines coins' in the bitcoin system—or issues instructions to carry out operations. In this respect, the 'physical' place of the data stored in a blockchain is irrelevant.
As a main rule, the authority to proceed in the data-protection supervision of the data controller using blockchain technology is the one on whose territory the data controller carries out the data processing operations, e.g. commands transactions, operates mining servers, etc.

With regard to cases related to international data transfer and cross-border data processing, the framework system for co-operation between the Members States of the European Union and their data-protection authorities is defined by Article 50 of the General Data Protection Regulation coming into force as of 25 May 2018.[10]

5) The Question of User Profiling in Relation to Blockchain Technology

With regard to the question whether the long-term use of the blockchain renders the monitoring of the user, the so-called profiling, possible, the Authority holds that this can only be judged in the all-round knowledge of the concrete system in question, including the data processed in them and the data processing operations related to them.

In respect of the personal data processed in a blockchain, the data controller must provide all-round information upon request by the data subject within 25 days under Section (1)[11]

[10]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[11]Section 15 (1) of the Privacy Act states: 'Upon the data subject's request the data controller shall provide information concerning the data relating to him, including those processed by a data processor on its behalf or according to his/her notice7, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities.' Relating to data processing, and - if the personal data of the data subject is made available to others - the legal basis and the recipients.

and (4)[12] of the Privacy Act. Under Section 15 (5) of the Privacy Act, the provision of information is free of charge for any category of data once a year. Additional information concerning the same category of data may be subject to a charge. The amount of such charge may be fixed in an agreement between the parties. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.

18 July 2017 at Budapest

Dr. Attila Péterfalvi
President, Hon.Univ.Professor

[12] Section 15 (4) of the Act states: 'Data controllers must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at the data subject's request, within not more than twenty-five days."