Publicēts:
Vilnius University. 7th International Conference of PhD Students and Young Researchers LAW 2.0. New Methods, New Laws. Conference Papers.
Vilnius: Vilnius University Press, 2019, 93.-102. p.

Mg. iur. Juris Janums
Assistant to sworn advocate
PhD student at University of Latvia

Risks related to the use of blockchain and the relevant criminal protection of the Criminal law in Latvia

Abstract

At the moment, in the recording of a transaction in the block chain there is no assessment made – whether it is good faith and whether the subject of the transaction is legal. Nor is the question of what data and in how wide peer-to-peer computer network to store. Thus, in his publication, the author to the described issues offers a view on criminal law protection of the use of a blockchain in Latvia, looking at issues such as the theft of financial identity, the protection of information to be transmitted, personal data, other data in the block chain as a subject of crime, as well as fraud cases related to the use of a blockchain and individual issues regarding criminally acquired or related to it property in the block chain. As a result, the author identifies some shortcomings and raises the question of the need to consider individual amendments to the Criminal Law in Latvia.

Keywords: blockchain, object of criminal offence, smart contracts, criminal law

Introduction

> «Blockchain is a data structure that is used to create a digital transaction ledger that, instead of resting with a single provider, is shared among a distributed network of computers. The result is a more open, transparent, and publicly verifiable system for digital transactions.»[1]

Although there are other explanations of the term of the blockchain, but their differences just seems different and they all contains the signs of the blockchain:

> «1) Structured data system (register or so called ledger);

[1] Database of Academy of Science of Latvia, http://termini.lza.lv/term.php?term=blokķēde&list=blokķēde&lang=LV, accessed on March 24, 2019

2) Contains information related to bilateral or multilateral transactions (incl. *bitcoin, cryptocurrency* and other transactions);

3) Being stored in a single distributed network of computers (*Peer-to-peer*).»[2]

One of the most common applications of blockchain technology is cryptocurrency.[3] It has been recognized in the legal literature, that

> «cryptocurrency is a commodity with a certain value, which is also a means of exchange, that encrypted with cryptographic methods is being kept in blockchain in memory of computer systems.»[4]

Thereby, cryptocurrency as a blockchain technology is potentially one of the most threatened blockchain technologies.

However, the technology of the blockchain in the field of information technology is increasingly being introduced in other applications, that are not related to a cryptocurrency. For example, an international information technology corporation «International Business Machines Corporation» (IBM) in September 2016 informed, that global banks and other financial institutions introduce blockchain technology in financial services systems faster as it was originally expected.[5] Similarly, the International Monetary Fund, in its January 2016 study, was focusing on the issues of smart contracts as a future form of transactions.[6] Furthermore in the legal periodicals, the digitized land registry[7] and even digitized arbitration process[8] stored in the blockchain has been already described.

Thus, due to the significant use of blockchain technology in the field of cryptocurrency, smart contracts, transactions and financial services, as well as in other areas, the question arises – whether the Criminal Law in Latvia contains the necessary criminal legal protection for the cases of block

---

[2] J. Janums, Blokķēdes krimināltiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums.

[3] Blockchain Top Trends In 201, https://channels.theinnovationenterprise.com/articles/blockchain-toptrends-in-2017, accessed on March 24, 2019.

[4] J. Janums, Jaunas kriptovalūtas emisija un tās kolektīvās finansēšanas krimināltiesiskie aspekti.[2018] LU 76. starptautiskās zinātniskās konferences rakstu krājums 417.

[5] J. Kelly, Banks adopting blockchain «dramatically faster» than expected: IBM, https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D, accessed on March 24, 2019.

[6] IMF staff discussion note. Virtual Currencies and Beyond: Initial Considerations. January, 2016, SDN/16/03, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf , accessed on March 24, 2019

[7] S. Lidere, Digitalizēts zemesgrāmatu reģistrs, kas balstīts uz blokķēdes darbības principiem, [2018] 47 (1053) Jurista Vārds

[8] L.L.Rieba, Blokķēdes tehnoloģijā balstīts šķīrējtiesas process, [2018] Jurista Vārds 47 (1053) Jurista Vārds

chain threats identified by the author previously[9] – i.e. with the existence and use of the blockchain related threats?

1. Legal threats related to use of the blockchain

One of the first threats blockchain technology developers name are the risks to the infrastructure necessary to the existence of the blockchain itself.[10] Since one of the features of the blockchain is that the system stores data in a decentralized network of distributed computers, thus - endangering the operation of the network and the operation of the computers in it, especially their availability to the computer network, threatens the blockchain itself.[11] Likewise, the operation of the blockchain system requires a stable computer operation, so also the operation of the computers in the blockchain itself is a threat object.[12] Thus, assessing the risks of the existence of a blockchain, it is necessary to analyze the related legal protection of computer and computer networks.

The second - legally much wider - range of threats is related to the use of block chain technologies, where, based on publications by industry experts[13], the main issues would be related to the nature and availability of information to be kept in the blockchain.

Accordingly, for example:

1) In the secure blockchain – sequential transaction records system – an illegal transaction is being recorded – it is understood to mean both transactions where the object of which is not permitted, such as drugs being bought at the *Dark Net / Dark Web* (dark net – peer-to-peer network with mutually limited and anonymous access)[14], or transactions related to money laundering, such as fraud, embezzlement and other illicit activities, for example bribe or illegal financing of political parties;

---

[9] J. Janums, Blokķēdes kriminālatiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[10] Bitcoin Developer Guide, https://bitcoin.org/en/developer-guide , accessed on March 24, 2019

[11] J. Janums, Blokķēdes kriminālatiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[12] Ibid.

[13] K. Iesalnieks, Blokķēdes tehnoloģija – mīti un patiesība par kriptorevolūciju, https://www.delfi.lv/news/versijas/kaspars-iesalnieks-blokkedes-tehnologija-miti-un-patiesiba-parkriptorevoluciju.d?id=49522737 , accessed on March 24, 2019

[14] Database of Academy of Science of Latvia, therm: Darknet, http://termini.lza.lv/term.php?term=darknet&lang=EN and https://en.oxforddictionaries.com/definition/darknet , accessed on March 24, 2019

2) In the secure blockchain personal data is being stored and subsequently processed in the manor that violates a person's right to privacy, which is furthermore stored on an unlimitedly distributed computer network.[15]

2. Legal protection of the blockchain in Criminal Law in Latvia

Taking into account the identified threats associated with the operation of the blockchain, for the protection of the interests of the operation of the blockchain in the Criminal Law in Latvia, we can mainly distinguish such groups of offenses:

1. Criminal offenses in the security of information systems – as the criminal offenses provided for in the Criminal Law as regards the existence of the blockchain itself, In turn, with regard to the nature and availability of information to be kept in the block chain, we can talk about such groups of criminal offenses:

2. Criminal Offences against Fundamental Rights and Freedoms of a Person,

3. Criminal Offences against Property, and

4. Criminal Offences in the field of Finance and Credit.[16]

2.1. Criminal offenses in the area of security of information systems regarding the existence of a blockchain itself

Criminal offenses in the area of security of information systems are included in the Criminal Law Chapter XX «Criminal Offences against General Safety and Public Order» and they are united by a common threat – group object – the general interest of security of the society. Thereby, taking into account, for example, data from the «*coinmarketcap.com*», where you can keep online track of changes in the value of more than 2'000 crypto currencies, the total value of cryptocurrency market at the moment (March 2019) has reached more than 120 milliard euros[17], as well as taking into account IBM observations on the widespread use of blockchain technologies in the field of financial services[18], it can be concluded that the use of blockchain technology at present and potentially in the future is very wide. Thereby based on the mentioned above, and taking into account one of the features of the blockchain technology – i.e., its existence on a wide spread computer network, – the

---

[15] J. Janums, Blokķēdes krimināltiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[16] Ibid.

[17] Cryptocurrencies by Market Capitalization, https://coinmarketcap.com/, accessed on March 24, 2019

[18] J. Kelly, Banks adopting blockchain 'dramatically faster' than expected: IBM, https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D, accessed on March 24, 2019

threat of the existence of a blockchain technology could jeopardize the general security interests and corresponds to the group object of interest of Chapter XX of the Criminal Law. Among other things, this is also confirmed by the example of the Estonian Central Depository «Nasdaq Estonia», where in the end of the 2016 they've successfully tested the blockchain technology in a electronic vote by shareholders meeting in an electronic environment, and it was recognized by the Stock Exchange as a sufficiently reliable, safe and usable technology for organizing general meetings of shareholders.[19]

However, looking at the specific criminal offenses, united by common threat object - Information Systems Security -, such as Arbitrary Access to Automated Data Processing System Pursuant to Section 241 of the Criminal Law, Interference of Operation of Automated Data Processing System Pursuant to Article 243 of the Criminal Law and Illegal Operations of Information Included in this System, Illegal Activities with Influential Devices Influenced pursuant to Section 244 of the Criminal Law, the acquisition, production, modification, storage and distribution of data, software and equipment provided for pursuant to Section 244.1 of the Criminal Law, as well as violation of the security rules of the information system provided for in Section 245 of the Criminal Law, we can observe, that the criminal offenses listed provide criminal protection for each element of the centralized computer system and for the system as a whole, but for the blockchain – as a decentralized peer-to-peer system – it is much more difficult to apply such sections of law.

For example, in the case of a centralized system, we can talk about a computer system where all information is centrally located in the memory of some computers (servers - network computers) with a single protection system, except for global information technology companies, which in one way or another, nevertheless, keeps different information in their dispersed centralized systems, it in different places in the world[20]. While, for example, in the case of cryptocurrency, the number of computers involved in the blockchain maintenance is measured in millions and stores all information in a single decentralized system. For example, as shown by the numbers of sells of the processors used for cryptocurrency mining in year 2017 more than 3 million units were sold[21]. So the size of the computers involved in the blockchain for providing a cryptocurrency system is measurable in millions. Moreover, unlike the centralized system architecture, where destroying any of its elements endangers the system as a whole, in case of a blockchain, to paralyze it, almost all the computers involved in the block chain should be destroyed, because each of the computers stores

[19] Nasdaq's Estonia E-voting Blockchain Solution, https://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html, accessed on April 15, 2019

[20] Google Data Centers, https://www.google.com/about/datacenters/inside/locations/index.html, accessed on April 15, 2019

[21] GPU market declined seasonally in Q4; cryptocurrency provides smaller offset as AIB prices rise, https://www.jonpeddie.com/press-releases/gpu-market-declined-seasonally-in-q4-cryptocurrencyprovides-smaller-offset, accessed on April 15, 2019

information about the entire system database, and thereby it is almost impossible to destroy.[22] Hence, damage to a single computer system (element) in a centralized system is more severe than damage to one computer from a million in a blockchain. Among the other things, it is often referred to in the various publications as one of the advantages of the blockchain technology.

It is therefore right to ask a question here – or, in the case of a threat to the computer system in the block chain, one can speak at all – of existence of an criminal offence – against the safety of the block chain operation? And, if we even refer to the criminal offenses currently provided for in the Criminal Law, are liability there isn't overly strict?

For example, currently disrupting the operation of an automated data processing system and unlawful action with information included in this system (Section 243 of Criminal Law) in accordance with Section 7, Paragraph three of the Criminal Law shall be considered a less serious crime (i.e. imprisonment for up to 2 years), but if a greedy intention has been identified (Section 243 Paragraph three of the Criminal Law), even as a serious crime (i.e. a sanction for imprisonment of up to 5 years).

But in the case of a blockchain – as mentioned above – technology itself excludes the possibility of manipulating the validity of the data contained therein, because every computer in the system keeps the system's current mirror image (copy), which at the same time completely eliminates the possibility of interfering with the operation of the blockchain system as a whole, compromising only one or a part of the system computers. Thereby interference of the blockchain in general is almost impossible, hence, compromising the small number of computers or a single computer in the blockchain, the qualifying characteristic of Article 243 of the Criminal Law does not materialize – i.e. interference of the operation of the system –, because as a whole, the system still continues to operate. But, if however, Article 243 of the Criminal Law is being applied in the case of a interference of a single computer in the blockchain, then, taking into account that the block chain still continues to operate, is a less serious crime shall not be considered as too severe classification for such criminal offence?

From the author's point of view, the problem of such regulation of the Criminal Law is related to it, for what kind of information technology architecture and industry rules the relevant norms were

[22] A. Dorri, M.Steger, S.S.Kanhere, R.Jurdak, BlockChain: A Distributed Solution to AutomotiveSecurity and Privacy [2017] 12/55 IEEE Communications Magazine

developed at the time of their adoption, because at that time no one predicted that once a group of people under the pseudonym Satoshi Nakamoto would offer the world a blockchain technology[23][24]

2.2. Criminal Offenses related to the use of the block chain

Offenses related to the use of the blockchain are mainly related to the nature and availability of information to be stored in the blockchain, where the author considers Criminal Offences against Fundamental Rights and Freedoms of a Person (Chapter XIV of The Criminal Law), Criminal Offences against Property (Chapter XVIII of The Criminal Law) and criminal offences in the field of finance and credit (Chapter XIX of The Criminal Law).[25]

So, when evaluating what data, how widely distributed computer network to store, and how to transfer and store them, it is reasonable to consider the criminal offenses provided in Chapter XIV of the Criminal Law, i.e. criminal offences against the fundamental rights and freedoms of the person, for example, such as Section 144, which provides for criminal liability for breach of the confidentiality of information transmitted over electronic communications networks and Section 145 of The Criminal Law, where criminal liability is provided for the illicit actions involving personal data. Initially looking at these offenses, the author has previously identified both the challenges of the General Data Protection Regulation[26] and relate to it Section 145 of The Criminal Law.

For example, what is the subject of a criminal offense in the case of breach of the confidentiality of information transmitted over electronic communications networks in case of «Monetizr», a Latvian startup registered in the US, that stores in a blockchain information about computer games players gaming habits in the US, and afterwards offers its to a computer games distributors and makers[27], or

---

[23] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, accessed on March 24, 2019

[24] J. Janums, Blokķēdes kriminmāltiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[25] Ibid.

[26] 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 [2016] OJ L 119/1 (General Data Protection Regulation)

[27] T. Zoldnere, Latvieši Silīcija ielejā: ar blokķēdes tehnoloģiju pēta datorspēlētājus, https://www.delfi.lv/bizness/tehnologijas/latviesi-silicija-ieleja-ar-blokkedes-tehnologiju-petadatorspeletajus.d?id=50818225, accessed on March 24, 2019

data on voters' political views, as it happened in the scandal of *Cambridge Analytica*[28], when such information was illegally transferred to political consulting companies.[29]

However, given the features of the blockchain technology described above, In the case of Article 144 of the Criminal Law it would be reasonable to ask a question, or the responsibility for the offenses contained therein could be at all, because the data in the blockchain is stored in the secure form of encryption. Thus, even if intercepted, they would not be usable, as long as the criminals do not have the user key (code), with which you can process encrypted information – incl. to read it. Thus, in relation to the criminal protection of correspondence as information on the blockchain could only be referred to as unfinished crimes. – i.i. their attempts – and only in very rare cases as completed crimes – as already mentioned, if the criminal has a decryption key (code).

In contrast, the main issue with the composition of the criminal offense under Article 145 of the Criminal Law, that could be related to the blockchain, is the nature of the data stored in the blockchain – i.e. what information should be kept in a publicly accessible and simultaneously encrypted block chain (i.i. to process). Likewise, no less important issue is related to the criminal protection in the space, but it is more of a jurisdictional issue that will not be dealt with this time. Thus the qualifying characteristics of Article 145 of the Criminal Law are the violation of a person's private life, which has caused significant damage.

However, as the Supreme Court of the Republic of Latvia rightly admits:

> «Not every violation of the rights guaranteed by the Republic of Latvia Satversme [Constitution] itself, without the evaluation of the violation, shall be considered a significant damage within the meaning of Article 23 of the Law «On the Procedure of Entry into Force and Application of the Criminal Law». Significant damage shall be determined on the basis of evidence verified by the court, assessing the nature, content, interest bearer, or the nature of the person at risk, and the attitudes towards the particular risk.»[30]

Therefore, the answer to the question - what information should be stored (i.e. processed) in a publicly available and at the same time encrypted blockchain system depends on the data subject's own attitude to the risk of the particular interest and should be assessed on a case-by-case basis.

---

[28] Ted Cruz using firm that harvested data on millions of unwitting Facebook users, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebookuser-data, accessed on March 24, 2019

[29] J. Janums, Blokķēdes krimināltiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[30] The decision of the Supreme Court of The Republic of Latvia of 29.09.2016. in case № SKK-190/2016 (11816003310), http://www.at.gov.lv/downloadlawfile/3640 , accessed on March 24, 2019

In turn, considering that the block chain can hold both the property itself and the right to such property, it is reasonable to look at the criminal offenses in Chapter XVIII of the Criminal Law against property. Such as The regulation of theft provided for in Article 175 of the Criminal Law, the regulation of fraud provided for in Article 177 of the Criminal Law, the regulation of fraud in the automated data processing system provided for in Article 177.1 of the Criminal Law, as well as the regulation of misappropriation provided for in Article 179 of The Criminal Law.[31]

Hence it is possible to immediately spot the characteristics of the blockchain, such as that it is not possible to steal the blockchain record as a property value itself, therefore, the Article 175 of The Criminal Law regarding the theft would not apply to it.

Similarly, the essence of the blockchain technology excludes false data entry to affect the block chain, as the block chain system allows recording only after the automated system has verified the accuracy of the data, therefore, the Article 177.1 of The Criminal Law regarding the fraud in the automated data processing system in essence, not even relevant to the blockchain. Conversely, in order to record a transaction in a block chain, an encryption key is required – which can be considered as an access right for each specific record – then you could reasonably talk about fraud.

Here, however, there is the question of financial identity theft and its association with fraud (Section 177 of The Criminal Law). You can also talk about fraud with system keepers, who by «mining» upkeeps the blockchain, such as company «BitFury», who receive a reward in a cryptocurrency for a «mining» and whose value is 400 million. USD[32] (Section 177 of The Criminal Law). Lastly, as with fraud, embezzlement can also be considered, for example, from the encryption key (code) providers and keepers (Section 179 of The Criminal Law)[33].[34]

Finally, although the legal definition of cryptocurrency in Article 2.2 of the Law on the Prevention of Money Laundering and the Financing of Terrorist Financing paragraph 2.2[35], as the legislator has clearly stated in Latvia, that it is a reflections of a value, but not the legal means of payment, at the same time in the light of the criminal offenses provided in The Chapter XIX of the Criminal Law in the field of Finance and credit, could expand the discussion on the cryptocurrency stored in the

---

[31] J. Janums, Blokķēdes krimināltiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[32] Bitcoin company made by Rigans valued at $400m, https://eng.lsm.lv/article/economy/economy/bitcoin-company-made-by-rigans-valued-at-400m.a261722/ , accessed on March 24, 2019

[33] J. Janums, Jaunas kriptovalūtas emisija un tās kolektīvās finansēšanas krimināltiesiskie aspekti. [2018] LU 76. starptautiskās zinātniskās konferences rakstu krājums 417

[34] J. Janums, Blokķēdes krimināltiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[35] Amendments of 26.10.2017. to a Law on the Prevention of Money Laundering and the Financing of Terrorist Financing of the Republic of Latvia, https://likumi.lv/ta/id/294868-grozijumi-noziedzigi-iegutulidzeklu-legalizacijas-un-terorisma-finansesanas-noversanas-likuma, accessed on March 24, 2019

blockchain as the subject of Article 193 of the Criminal Law, because, as it is well known you can pay for goods and services by the cryptocurrency like as by legally defined means of payment. In addition, it would be worthwhile to discuss the data in the blockchain as such, and it would be reasonable to ask the question - whether theft or the stealing of the payment instrument from the blockchain would be realistic or have a different objective expression.

It would also be reasonable to ask the question about Article 193.1 of the Criminal Law – regarding the acquisition, production, distribution, use and storage of data, software and equipment for illegal activities with financial instruments and means of payment, not only the question of obtaining access data for cryptocurrency wallet with encryption keys, but also with regard to software aimed at destroying, blocking and, in this case, competing with the provisions of the offense referred to in Section 244 of the Criminal Law.[36] In the view of the author, the value of the cryptocurrency as an element of the blockchain with the property value is to be recognized as a means of payment within the meaning of Article 193 of the Criminal Law.[37]

Thus, taking into account, for example, the size of the cryptocurrency market, it would be reasonable to consider whether the liability for the risks is high enough, or whether it would be necessary to supplement the Criminal Code with the financial and credit composition of the offenses that would also include liability for special entities. That provides the circulation of specific blockchain technology data to its users, such as cryptocurrency developers or cryptocurrency exchange keepers. For example, the news about the cryptocurrency exchange «QuadrigaCX», which is the largest cryptocurrency exchange in Canada, has recently alarmed the world, when its main developer died, the access to property – in electronic form – with value of 190 million USD is being lost, because only the developer alone knew encrypted access code to those transactions.[38] Thus, the legislator should consider the need to regulate security requirements in the relevant sphere and to provide for such cases responsibility in the Criminal Law.

Conclusions

[1] The threat to the existence of blockchain technology is consistent with the threat to the general security interests and hence corresponds to the interest of the group protected under Chapter XX of the Criminal Law.

---

[36] J. Janums, Blokķēdes krimināltiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums

[37] Ibid

[38] Cryptocurrency investors locked out of $190m after exchange founder dies, https://www.theguardian.com/technology/2019/feb/04/quadrigacx-canada-cryptocurrency-exchangelocked-gerald-cotten, accessed on March 24, 2019

[2] Damage to a single computer system (element) in a centralized system is significantly more severe than the damage that can be caused to one computer from a million in the blockchain system.

[3] Interference of some of the computers in the blockchain system does not damage the operation of the blockchain, hence the qualifying feature of Article 243 of the Criminal Law – interference of the operation of the systems – does not occur, because in this case the system continues to operate as a whole.

[4] Offenses related to the use of the blockchain are mainly related to the nature and availability of the information to be kept in the blockchain.

[5] As regards the criminal protection under Article 144 of the Criminal Law of correspondence as information on the blockchain, could only be referred to as an unfinished crimes – i.i. their attempts – and only in very rare cases as completed crimes – i.e. in cases if the criminal has a decryption key (code).

[6] The question of what information should be stored (i.e. processed) in a publicly available and at the same time encrypted blockchain depends on the data subject's ownattitude to the risk of the particular interest and should be assessed on a case-by-case basis.

[7] Thus, the legislator should consider the need to regulate security requirements in the sphere of cryptocurrency developers and cryptocurrency exchange keepers, and provide for such cases necessary responsibility in the Criminal Law, which is not currently provided for in the Criminal Law.

Bibliogaphy

1. A.Dorri, M.Steger, S.S.Kanhere, R.Jurdak, BlockChain: A Distributed Solution to Automotive Security and Privacy [2017] 12/55 IEEE Communications Magazine
2. Amendments of 26.10.2017. to a Law on the Prevention of Money Laundering and the Financing of Terrorist Financing of the Republic of Latvia, https://likumi.lv/ta/id/294868-grozijumi-noziedzigi-iegutu-lidzeklu-legalizacijas-unterorisma-finansesanas-noversanas-likuma, accessed on March 24, 2019
3. Bitcoin company made by Rigans valued at $400m, https://eng.lsm.lv/article/economy/economy/bitcoin-company-made-by-rigans-valuedat-400m.a261722/ , accessed on March 24, 2019
4. Bitcoin Developer Guide, https://bitcoin.org/en/developer-guide , accessed on March 24, 2019
5. Blockchain Top Trends In 201, https://channels.theinnovationenterprise.com/articles/blockchain-top-trends-in-2017, accessed on March 24, 2019
6. Cryptocurrencies by Market Capitalization, https://coinmarketcap.com/, accessed on March 24, 2019
7. Cryptocurrency investors locked out of $190m after exchange founder dies, https://www.theguardian.com/technology/2019/feb/04/quadrigacx-canadacryptocurrency-exchange-locked-gerald-cotten, accessed on March 24, 2019

8. Database of Academy of Science of Latvia, http://termini.lza.lv/term.php?term=blokķēde&list=blokķēde &lang=LV, accessed on March 24, 2019
9. Database of Academy of Science of Latvia, therm: Darknet, http://termini.lza.lv/term.php?term=darknet&lang=EN and https://en.oxforddictionaries.com/definition/darknet , accessed on March 24, 2019
10. Google Data Centers, https://www.google.com/about/datacenters/inside/locations/index.html, accessed on April 15, 2019
11. GPU market declined seasonally in Q4; cryptocurrency provides smaller offset as AIB prices rise, https://www.jonpeddie.com/press-releases/gpu-marketdeclined-seasonally-in-q4-cryptocurrency-provides-smaller-offset, accessed on April 15, 2019
12. IMF staff discussion note. Virtual Currencies and Beyond: Initial Considerations. January, 2016, SDN/16/03, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf , accessed on March 24, 2019
13. J. Janums, Blokķēdes krimināltiesiskās aizsardzības aspekti. [2019] LU 77. starptautiskās zinātniskās konferences rakstu krājums
14. J. Janums, Jaunas kriptovalūtas emisija un tās kolektīvās finansēšanas krimināltiesiskie aspekti. [2018] LU 76. starptautiskās zinātniskās konferences rakstu krājums 417
15. J. Kelly, Banks adopting blockchain 'dramatically faster' than expected: IBM, https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D, accessed on March 24, 2019
16. K. Iesalnieks, Blokķēdes tehnoloģija – mīti un patiesība par kriptorevolūciju, https://www.delfi.lv/news/versijas/kaspars-iesalnieks-blokkedestehnologija-miti-un-patiesiba-par-kriptorevoluciju.d?id=49522737 , accessed on March 24, 2019
17. L.L.Rieba, Blokķēdes tehnoloģijā balstīts šķīrējtiesas process, [2018] Jurista Vārds 47 (1053) Jurista Vārds
18. Nasdaq's Estonia E-voting Blockchain Solution, https://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-Evoting-Nasdaq-Believes-So.html, accessed on April 15, 2019
19. 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 [2016] OJ L 119/1 (General Data Protection Regulation)
20. S. Lidere., Digitalizēts zemesgrāmatu reģistrs, kas balstīts uz blokķēdes darbības principiem, [2018] 47 (1053) Jurista Vārds
21. S.Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, accessed on March 24, 2019
22. T. Zoldnere, Latvieši Silīcija ielejā: ar blokķēdes tehnoloģiju pēta datorspēlētājus, https://www.delfi.lv/bizness/tehnologijas/latviesi-silicija-ieleja-arblokkedes-tehnologiju-peta-datorspeletajus.d?id=50818225, accessed on March 24, 2019
23. Ted Cruz using firm that harvested data on millions of unwitting Facebook users, https://www.theguardian.com/us-news/2015/dec/11/senator-tedcruz-president-campaign-facebook-user-data, accessed on March 24, 2019
24. The decision of the Supreme Court of The Republic of Latvia of 29.09.2016. in case № SKK-190/2016 (11816003310), http://www.at.gov.lv/downloadlawfile/3640 , accessed on March 24, 2019