JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2019 December Volume 9 Number 2
http://doi.org/10.9770/jssi.2019.9.2(2)

Scopus®

TOWARDS SUSTAINABLE CRYPTOCURRENCY: RISK MITIGATIONS FROM A PERSPECTIVE OF NATIONAL SECURITY

Tadas Limba[1], Andrius Stankevičius[2], Antanas Andrulevičius[3]

[1,2,3] Mykolas Romeris University, Ateities str. 20, Vilnius, Lithuania

Emails: [1]tlimba@mruni.eu; [2]stankevicius@mruni.eu, [3]antanas@fin.lt

Received 14 March 2019; accepted 15 September 2019; published 15 December 2019

Abstract. Cryptocurrency market is developing fast during the past few years. Cryptocurrency now is available as a form of payment for retail goods, as an instrument for a wholesale international transaction a mean of exchange for whatever goods and is available through ATM's. Moreover, it is developing as a possibility for fundraising a) as a private debt b) as seed capital. Companies like Facebook are discussing launching own cryptocurrency. Bank UBS is developing its blockchain based virtual currency as well. However, scientist agrees that cryptocurrency has an important impact to national security. It became a relevant instrument for illegal good transactions, a mean of exchange in the darknet and an instrument for money laundering or infrastructure for new kind of money-laundering practices (for example- "Smurfing" phenomena (EU Observer, 2019)) European Union is launching AML and KYC procedures for the cryptocurrency market. Would it be efficient? Why are we implementing KYC and AML procedures for cryptocurrency? Is it able to minimize risks?

Keywords: cryptocurrency; know your customer; anti-money laundering; national security

Reference to this paper should be made as follows: Limba T., Stankevičius A., Andrulevičius A. 2019. Towards sustainable cryptocurrency: risk mitigations from a perspective of national security, *Journal of Security and Sustainability Issues* 9(2): 375-389. http://doi.org/10.9770/jssi.2019.9.2(2)

JEL Classifications: O33

Additional disciplines law, sociology

1. Introduction

The cryptocurrency market is developing. Within eleven years there are 2290 know cryptocurrencies worldwide (www.coinmarketcap.com 2019), which is 12 times more compared to 180 official currencies (Swiss Association for Standardization, 2019).

While the inventor of first cryptocurrency Bitcoin, Satoshi Nakamoto, was anonymous, currently world recognized people and companies are eager to issue Initial Coin Offering (hereinafter - ICO). A group of financial firms lead by UBS bank is planning to launch their digital currency, based on blockchain (The Economist 2019), Facebook is launching its cryptocurrency called Libra (The Guardian, 2019).

During past few years, Banking sector revealed, that the system is not efficient enough to implement strict Know Your Customer (hereinafter – KYC) and Anti-Money Laundering (hereinafter – AML) regulations and to prevent the financial system from foreign threats (Barone, Masciandaro 2019; Kordík, Kurilovská 2017; Šimonová, et al. 2019). There were number of cases in Big Scale (Danske Bank 230 billion USD, Swedbank 10 billion USD) and Small scale 4 million USD (Smurfing case in Belgium) (Bloomberg 2019, Bloomberg 2019, EU Observer

2019). Two different approaches of money laundering cases: a) money laundering wholesale, working through several intermediaries with especially big amounts b) money laundering partitioning, when laundered money is divided in small partials to prevent the attention of regulators; shows that the system is not efficient enough.

Limba et al. (2019a, 2019b) define cryptocurrency as infrastructure for critical infrastructure. Therefore the dependence on the quality of the infrastructure for critical infrastructure brings quality for the exact society that is using exact infrastructure. Cambel et al. (2017). The fragility and importance of critical infrastructure are stressed by Tvaronaviciene (2018a, 2018b) as well - "Enhanced resilience of society to critical infrastructure infringement is and the ultimate goal of fostering of leadership for critical infrastructure protection.

The main point of discussion in current time- does cryptocurrency need to regulate by law norms, or it will realize through self-regulation? Another question – would cryptocurrencies make the financial infrastructure weaker and deliver more threats to it? Or is cryptocurrency a tool to evade KYC and AML procedures? Therefore it is important to discuss possible ways of cryptocurrency impact to national security and ways to mitigate risks.

Actuality – The European Union is preparing a legal framework for cryptocurrency regulation. Many countries are discussing possible regulations to minimize risks in cryptocurrencies. The actuality of the topic is highly important to discuss risks that cryptocurrency brings to national security.

Authors analyze cryptocurrency phenomena through risk mitigation, which reduce the possible threat to national security. Based on the results of expert interview, the possible interaction between cryptocurrency and AML/ KYC procedures were analyzed.

Scientific issue – cryptocurrencies are part of global finance, with the relevant amount of turnover and asset value allocated, however AML and KYC procedures for cryptocurrencies transaction number still in the process of discussion.

The object of the topic – KYC and AML procedures versus cryptocurrency: the context of national security.

The aim of the paper to disclose possible mitigations of cryptocurrency risks to national security, using KYC and AML procedures.

The **main tasks** of the topic are as follows:
1. To reveal the importance and the need of cryptocurrency as an infrastructure quality improvements;
2. To discuss the need for KYC and AML implementation for cryptocurrency;
3. To emphasize obstacles and challenges for KYC and AML implementation for cryptocurrencies

Methodology:

- The method of document analysis was used: selected and analyzed scientific literature, legal documents, and expert conclusions. The literature was selected based on keywords from reliable sources of information (monographs, peer-reviewed scientific journals, information accesses of state institutions). Data analyzed by *content* analysis.
- The linguistic method was applied to identifying the content of concepts and definitions.
- The systematic method revealed cryptocurrency phenomenon as a digital representation of value, which is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.
- The methods of critical-analytical and comparative analysis were applied to formulating interim and final conclusions.
- An expert interview was conducted to reveal systemic, in-depth features of the cryptocurrency phenomenon.

2. Literature review

For literature review authors have chosen few lines to discuss a) cryptocurrency risk to national security b) the importance of cryptocurrency environment quality c) the integrity of cryptocurrency and shadow economy d) ways to improve cryptocurrency quality from a perspective of national security e) challenges regulating cryptocurrency.

Cryptocurrency risks to national security. According to Tvaronaviciene (2018), cybersecurity threats to national economies has a wide range of facets as: a) internet and terrorism b) exploitation of social networks for various purposes b) manipulation of voting c) attack on institutions of critical importance. Limba et al. (2019a, 2019b) state that cryptocurrency influence national security in various ways. The matrix influence reflects the depth and volume of the interaction of cryptocurrencies and national security. As cryptocurrency is the infrastructure for critical infrastructure from a perspective of cyber threats it is critical infrastructure for digital shadow economy (Table 1).

Table 1. Cryptocurrency threat to National Security risk classification

<table>
<tr><th colspan="2">I. Crypto currency as an infrastructure for criminal activity</th><th colspan="2">II. Threats to economic security</th><th colspan="2">III. Threats to public security</th></tr>
<tr><td rowspan="3">1. A tool for criminal activity</td><td>A. An Internet platform for drug dealers</td><td rowspan="3">1. Direct forms</td><td>A. Illegal trade activity</td><td rowspan="3">1. Direct forms</td><td rowspan="3">A. Organized crimes:
• drug trafficking;
• crime (illegal. activity;
• money theft;
• criminal fraud;
• tax evasion and tax fraud.</td></tr>
<tr><td>B. Illegal trade in wide meaning</td><td>B. Tax evasion:
• illegal finance-banking activity;
• money laundering;
• tax fraud;
• money transit.</td></tr>
<tr><td>C. Tax evasion:
• money laundering;
• money layering;
• money transit.</td><td>C. Corruption.</td></tr>
<tr><td rowspan="3">2. As an object of criminal activity</td><td>A. Money theft</td><td rowspan="3">2. Indirect forms</td><td>A. Competitiveness</td><td rowspan="3">2. Indirect forms</td><td>A. Financing terrorism</td></tr>
<tr><td>B. Criminal fraud activity</td><td>B. Social exclusion</td><td>B. Hybrid threats</td></tr>
<tr><td>C. Corruption</td><td>C. Non-transparent lobbying activity
D. Trust in the government</td><td>C. Threats to the objects of a critical infrastructure</td></tr>
</table>

Source: Limba et al. (2019)

According Limba et al. (2019), cryptocurrency as infrastructure brings the following potential risks: a) money theft, b) a lack of arbitrage, c) money laundering, d) tax avoidance, e) financing terrorism. Tvaronaviciene (2018) states "main efforts should be taken to provide security for their critical infrastructure because only this can ensure the wellbeing of the country and its people".

The importance of cryptocurrency environment quality. According to Tvaronaviciene (2018) "contemporary environment in conditions of globalization predicting of development peculiarities and external factors' impact becomes an especially urgent issue". Stankevicius et al. (2018) stated, that "critical infrastructure system has a dynamic, evolutionary character in the context of social change"

The integrity of cryptocurrency and shadow economy. Limba et al. (2019a) state "negative factors of cryptocurrency are typical (homogeneous) for most countries". If negative factors are homogenous, ways to mitigate negative factors are homogenous as well. Besides urgency globalization brings need to cooperate building and fulfilling norms of activities as Štitilis et al. (2016) stress the importance of cybersecurity international integrity

development. Scientists emphasize that cybersecurity shall be developed in two levels: 1) locally 2) global cooperation of cybersecurity development. Desmond et al. (2019) findings are that "the cryptolaundering process is considered to be a complex socio-technical system". Novikovas et al (2017), states, that "countries must feel concern regarding consolidation of their security". However despite the need of global integrity and cooperation according to Zetzsche et al. (2018) "There is a strong differentiation of treatment among countries and low levels of legal certainty".

Ways to improve cryptocurrency quality from a perspective of risks to national security. Limba et al. (2019) state that lack of AML and KYC procedures in cryptocurrency case increase terrorist act risk. Therefore it is essential systematically develop research interaction between disruptive technologies (including Bitcoin – authors remark) and cybersecurity. Barone et al. (2019) and Danton (2014) determines anonymity and lack of control as a key money laundering elements. Clayton (2018) as a chairman of US Securities and Exchange Commission determined that KYC and AML procedures should be a must for ICO.

Challenges regulating cryptocurrency. Tkachenko et al. (2019) define that in Bitcoin – based system there is no possibility to ban the transfers immediately; there is only a possibility to regulate intermediaries or to implement penalties after the transactions are done. Authors identify as well, that Bitcoin – based system is a new type of financial infrastructure, therefore a new type of lawmaking and law enforcement is needed. Tu et al. (2015) after modelling cryptocurrency under existing US framework came to the conclusion that the development of an efficient regulatory regime for cryptocurrencies requires great interagency communication of regulatory consideration raised by virtual currency.

Also mentioned, that cryptocurrency is an infrastructure for new kind of money – laundering practices. In one hand ES brings sanctions for some subjects, outside EU borders, but now day exist paradox - "dirty" money layout in EU countries.

Money launderers break down a large amount of money into smaller chunks and have associates known as "Smurfs" deposit the funds in different accounts in different places. For example Belgium case: to avoid transparency, the criminal group paid out in sums of €10,000 to €120,000 to Belgian suppliers of construction materials and engineering equipment, such as flooring, heating, lighting, and ventilation systems (EU Observer, 2019).

Summarizing we can state that cryptocurrency as critical infrastructure for critical infrastructure and critical infrastructure for digital shadow economy. The quality of cryptocurrency environment is high importance and urgency, therefore, risk mitigations should be implemented to improve its quality and to prevent risks that could have long-term impact on certain society. Despite the need for global cooperation implementing efficient instruments to improve the national security environment, there is a lack of Instruments for cryptocurrency quality improvement should be implemented globally to be efficient enough.

3. Qualitative Analysis of Cryptocurrency as a Threat to National Security

3.1. Research Methodology

The **main tasks** of the **research** are as follows: to analyze cryptocurrency as an instrument for money laundering, influencing national security from a practical professionals point of view, the authors applied The interview method. Qualitative analysis pros: deep and detail; openness to generate new ideas and theories; opportunity to see the world through investigator position and opportunity to avoid prejudices.

The cons of the study: difficult to structure and to generate received data; the study is strongly dependent on investigators experience, abilities and skills, which is impossible to measure.

Cohen, Manion (1989), Tidikis (2003) indicates a threefold purpose of the research interview method:

1. Direct tool to get the required information.
2. Measure the hypotheses raised in check.
3. Interview in conjunction with other methods can be used to gather information and consideration of other methods.

Interview object: a) cryptocurrency as social phenomenon b) cryptocurrency as an infrastructure influencing national security c) perceived ways to minimize risks carried by cryptocurrency c) determine either the perceived view of top position people has the same direction.

The interview was followed by quality criteria of Kvale (1996):

a) The extent of spontaneous, rich, specific, and relevant answers from the interviewee.
b) The shorter the interviewer‘s questions and the lauder the interviewer‘s answers, the better.
c) The degree to which the interviewer follows up and clarifies the meanings of the relevant aspects of the answers.
d) The ideal interview is to a large extent interpreted throughout the interview.
e) The interviewer attempts to verify his or her interpretations of the subject’s answers in the course of the interview.

The interviews were made in July 2019. Four interviews lasted about 60 minutes, one interview – 30 minutes. Before the interview, the interviewers were explained about the research object and the context. The interview is ‘self-communicating’ – it is a story contained in itself that hardly requires much extra descriptions and explanations.

According to Crouch et al. (2006), “Small number of cases will facilitate the researcher’s close association with the respondents, and enhance the validity of fine-grained, in-depth inquiry in naturalistic settings”. Libby and Blashfield maintain the same position. Cohen et al. (2007) keep a position that “the interviewer will need to establish an appropriate atmosphere such that the participant can feel secure to talk freely”. To prevent political speculations, to reach higher transparency of interviews and to get open position on the cryptocurrency the interviews are anonymous. Respondents were informed about interview confidentiality and the interview was not recorded. Also according to Kvale (1996) “the researcher is the research instrument, the effective interviewer is not only knowledgeable about the subject matter but also an expert in interaction and communication”. Therefore most of the interviews were structured as informal. During the interview, a few topic lines were developed to reveal problematic issues. All participants were willing to assist in the investigation.

The interview was started from the respondent opinion about the cryptocurrency itself, to get main ideas the way the respondent sees cryptocurrency and to get the most open view on cryptocurrency. Latter respondents were asked to identify potential risks that cryptocurrency can bring in terms of money laundering and the threat to national security. At the end of the identification of cryptocurrency risk, the position regarding cryptocurrency regulation was asked to be determined, to get an overall view of the interviewee. All respondents were asked the same questions.

Received information was analyzed applying *content analysis* method. Content analysis is a procedure for the categorization of verbal or behavioral data, for purposes of classification, summarization, and tabulation. According to Wamboldt B.D. (1992), “content analysis has external validity as a goal. Because of its focus on human communication, the content analysis offers practical applicability, promise, and relevance for research.”

3.2. Characteristics of elements participating in interview

For the interview, we were targeting top position individuals involved in Banking, Legislation (National Security) and cryptocurrency operations activity. All respondents run top positions, participates in political and social activity. One respondent is actively performing in the cryptocurrency market and is an owner of the company, which listed ICO.

The structure of the interview was based on the literature review. However, the main goal was to get an individual view on cryptocurrency, the depth of understanding it as a product, the individual understanding as a threat to national security and the perceived need to regulate it.

Two participants are financial industry professionals and have high cryptocurrency. Both participated in international and local conferences. Both respondents are well informed about existing regal regulations concerning cryptocurrency and participate in discussions to regulate it.

One participant has an extremely deep understanding of cryptocurrencies. The participant has activity in mining, selling, trading, arbitraging from cryptocurrencies and issuing ICO. The respondent is familiar with banking rules for KYC and AML applied for customers as well.

It is important to mention that one participant has a rather modest understanding of cryptocurrency. He stated that during Parliament work he did not participate in any discussion or any report for government institution related to external, internal threats were not discuses. However, the responded stated that he had participated in an international security conference where the discussion took place about cryptocurrency as a threat to national security. Therefore he assumes cryptocurrency potential having an impact to national security.

To obtain information from a wider circle of participants who are concerned with cryptocurrency, interviews were interviewed persons whose activities are related to legislation and practice activities (see Table 2, Table 3).

Table 2. The Sample Description

Group	Occupation	Working experience	Approximate age and sex	Means of Interview
Banking	CEO/OWNER	Bank activity supervision including operations, KYC and AML compliance	Man, about 35 years	Face-to-face
Banking	CEO	Actively participates in Banking sector lobbying including legislation and regulation	Man, about 47 years	Face-to-face
Cryptocurrencies	CEO/OWNER	Owner of company which has listed own cryptocurrency	Man about 28	Face-to-face
Legislator	Member of Parliament	Legislator, participant of National Security Committee	Man, about 55 years	Face-to-face
Legislator	Member of Parliament	Legislator, participant of National Security Committee	Man, about 37 years	Face-to-face

3.3. Interview results

Table 3. Grouped Data Obtained During the Interviews

Storyboard	Examples of interview
Position regarding cryptocurrency as money laundering instrument	"Cryptocurrency – the main instrument for money-laundering"
	"No control during cross border transactions"
	"No paths of transaction"
	"Cryptocurrency – an instrument for illegal activity"
	"Cryptocurrency – is used for money-laundering cases"
	"Custom does not check if You have virtual wallet with 100 million USD when You travel"
	"Instrument for money-laundering"
	"No data is reported to crime prevention organizations about cryptocurrency transactions "
	"In case of money laundering investigation in cryptocurrency case is hard to get data about participants and transactions"
	"If someone is virtual millionaire in cryptocurrency he or she would need to convert money into real money to buy real things (houses, cars fancy things). Then the information is gathered, and checked the source of money origin"
	"Money laundering is mitigated when cryptocurrency is converted to real money and/or buying real estate or assets that are under register"
	"Cryptocurrency is a "grey zone" area with uncontrolled and unknown activity and participants (authors remark)"
Respondent view on Cryptocurrency as a Risk to National Security	"The black market in the internet is based on cryptocurrencies"
	"Using cryptocurrency as a mean of payment, illegal things are available to buy"
	"Cryptocurrency bring risk to national security, tax evasion, illegal good transit"
	"Cryptocurrencies are used as an for Blackmailing "
	"Cryptocurrency is not a threat to national security itself but it is the threat the way it is adopted"
	"Illegal activities and organized crime is strongly using cryptocurrency as a mean of transaction therefore it brings a lot of risks to national security"
	Black market is based on crypto currencies
	"Cryptocurrency might be used as an instrument to induce chaos in the country"
	"Cryptocurrency bring risk to national security"
	"Risk to national security is seen as a risk to financial security which is considered as low"
	"Perceives cryptocurrency as an instrument for terrorist activity"
	"Risk mitigator is the place where cryptocurrency holder wants to exchange his virtual assets to FIAT currency"
Perceived respondent view on cryptocurrency regulation	"Regulation is necessary", "big scale of people who would be negatively affected"
	"The KYC procedure during cryptocurrency account opening do not prevent from further money laundering, as accounts can controlled by third parties"
	"Local regulation would not be efficient unless regulation is implemented in comparing relevant part of states"
	"The right of cryptocurrency issuance should be controlled by the governemnt, who has a right to issue money"
	"High need to regulate cryptocurrency market"
	"The question is who would be eligible to regulate cryptocurrencies and in what way"
	"No one can stop Bitcoin transactions as it is virtual data flow performed autonomously"
	"Bitcoin can be allowed or forbidden but no regulation is possible due to its nature of autonomy"
	"Exchange markets should take position of gathering information, making KYC and AML procedures"
	"No need to regulate cryptocurrencies" "It would be regulated within existing legislation when converting cryptocurrency to FIAT currency"
	"Local cryptocurrency regulation would not be efficient as it is a global product"
	"Possible cryptocurrency regulation not earlier than in ten years"
	"The necessity to regulate is a matter of time"
Other aspects of discussion arisen from the interview	"If people who pay 10 000 EUR for Bitcoin – pay for anonymity, then it is a huge bubble"
	"The cryptocurrency price is based on global community answers to following questions: a) Is it legible to claim state write to issue money b) Is the value of cryptocurrency is reasonable c) Cryptocurrency regulation leads to state exclusivity for cryptocurrency issue"
	"Cryptocurrency value is based on speculations"

Source: Respondent Interview made by authors

3.3.1 Thematic-study topic: cryptocurrency is an infrastructure for money laundering

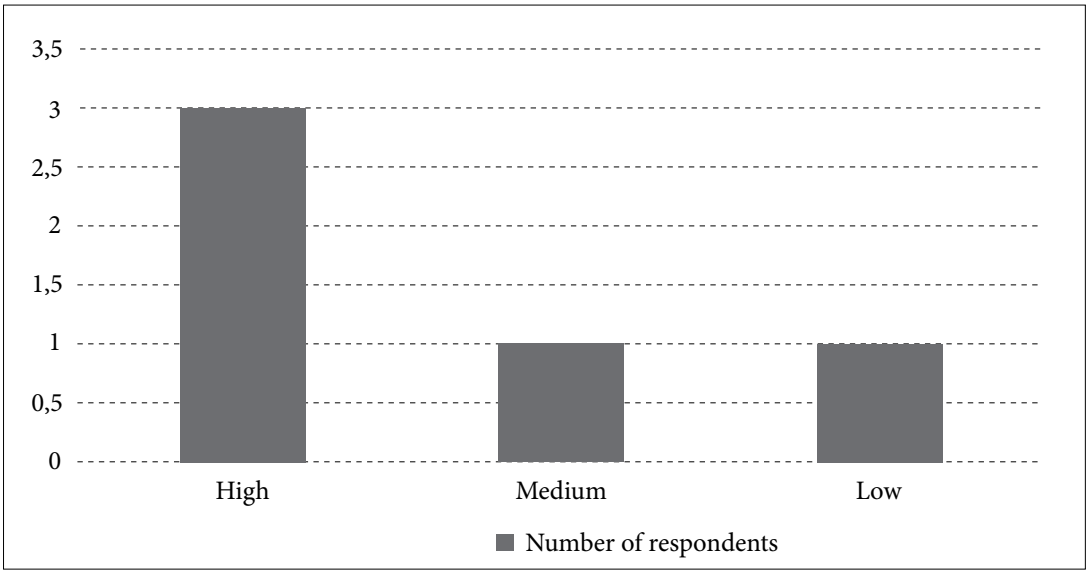
All participant see cryptocurrency as the main instrument for money-laundering. Respondent mention cross border transactions as important risk carriers as they see cryptocurrency as riskier than cash money as there is no custom to check international money flows. The position is supported by Financial Crimes Investigations Bureau - cryptocurrencies are obtained virtually, therefore, counterparties do not need to meet fiscally, therefore it is an attractive instrument for fraud cases, money laundering and legalization for illegal money (www.Alfa.lt 2018).

The importance of money laundering is also related to investigations of money laundering cases. Due to cryptocurrency origin, it is hard to determine its path and the origin it comes. Government institutions do not record or gather information about cryptocurrency transactions. The same as money laundering investigations, which are difficult, due to information limitations.

3.3.2. Thematic-study topic: cryptocurrency brings risk to national security

All respondents have common strategic view that cryptocurrencies are a threat to national security. However the extent of risks is considered to be the area of discussion (Table 4).

Table 4. Respondent opinion weather cryptocurrency brings threat to national security



Source: Respondent Interview made by authors

Although all participants agree that cryptocurrency is a mean of exchange in Black Market and instrument to buy illegal things, there was only one position saying that controlling exchange houses of cryptocurrencies to FIAT currencies, would be relevant risk mitigator to prevent crimes.

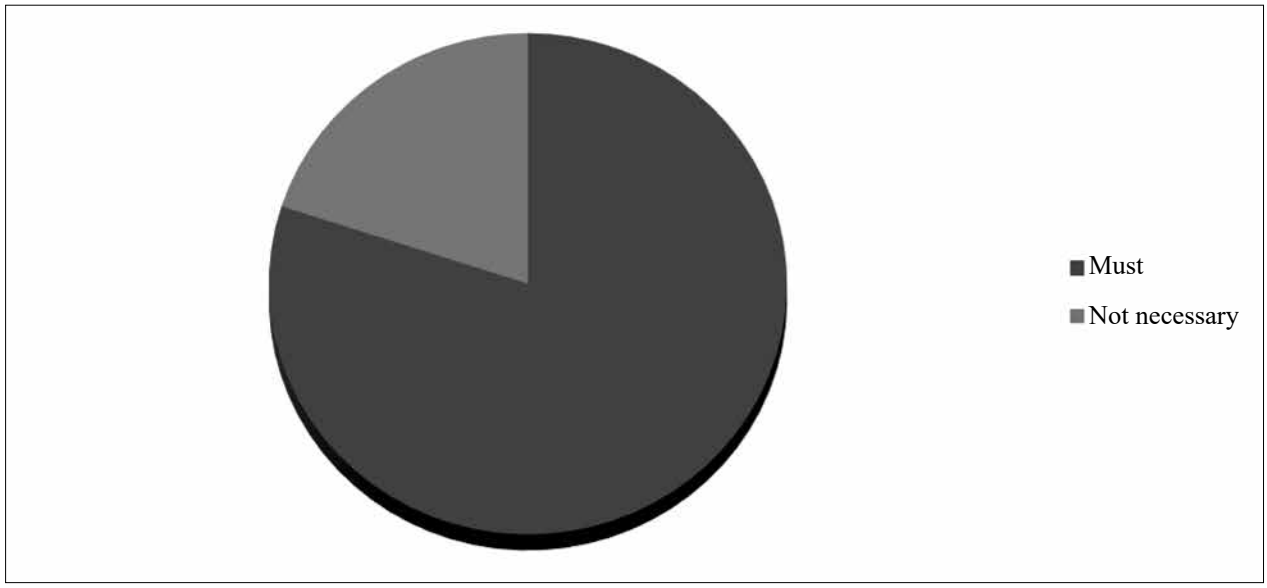
Institutions highlight the relevance of cryptocurrency as a threat to national security as well (The President of the United States, 2017), Lithuanian Bank (2017) declares that “In no mean we cannot create the illusion that cryptocurrencies are maintained by the bank and therefore safe” and “the participants of the financial sector should not participate in cryptocurrency selling, they should ban their customers to use cryptocurrency as a mean of payment”. International cryptocurrency transactions show possible users from high-risk countries (Siria, Iraq, Iran, Jamen, Tunisia and etc) and high-risk users (members of criminal cartels, terrorists), states Financial Crime Investigation Bureau (www.Alfa.lt 2018).

3.3.3. Thematic-study topic: Possibilities to regulate cryptocurrency

Four out of five respondents see the need to regulate crypto currencies. One is considering that existing regulations are enough as, despite obstacles to get information about cryptocurrency holders, there is always a way to control the origin of money.

Important to mention that part of respondents were rather pessimistic in KYC and AML procedure implementation for cryptocurrencies due to: a) possible transfer of accounts to third parties b) it is impossible to stop cryptocurrency transactions c) local or fragmented regulation would not be efficient for a global IT product d) unclear regulators for the instrument (Table 5).

Table 5. Respondent Opinion on Need to Regulate Crypto Currencies



Source: Respondent Interview made by authors

3.4. Generalizations

Respondent statement data analysis disclosed consistency of respondent opinions, and revealed the following guidelines for discussion:

1. All participants agree that cryptocurrency is an infrastructure for money laundering. The scale and depth of discussion about the ways money can be laundered through cryptocurrency dependent on understanding the way cryptocurrency operations can proceed. The more respondent was aware of cryptocurrency operations the more

2. All participants agree that cryptocurrency is a threat to national security. All participants named one or few risks that cryptocurrency brings to national security.

Summarizing respondent position it is obvious that the respondent has a homogeneous view on cryptocurrency as an instrument for money laundering and as a threat to national security. The homogeneity is based on the following factors presented below (Table 6).

Table 6. Research outcome summary

National security	From money laundering aspect
I Anonymity	
a) Illegal good trade	a) No paths of transaction
b) Tax evasion	b) Equivalent of cash money
c) Blackmailing keeping the confidentiality of the criminal;	
II Lack of transaction control	
a) No ability to stop illegal operations	a) No cross border transaction control
b) Tax evasion	b) No paths of transaction
c) Instrument to induce chaos in the country	c) No transaction data reported to institutions
d) Potentially able to influence financial market stability	

Source: Respondent Interview made by authors

Therefore the finding are that cryptocurrency as a threat for national security and money laundering cases, value drivers are I) anonymity II) lack of transaction control.

4. KYC and AML Practical Adoption in Banking Sector and for Crypto Currencies

Developing risk mitigations for the cryptocurrency market it is relevant to the overview Banking sector, therefore, it is relevant to make an overview of the Banking sector regulatory framework.

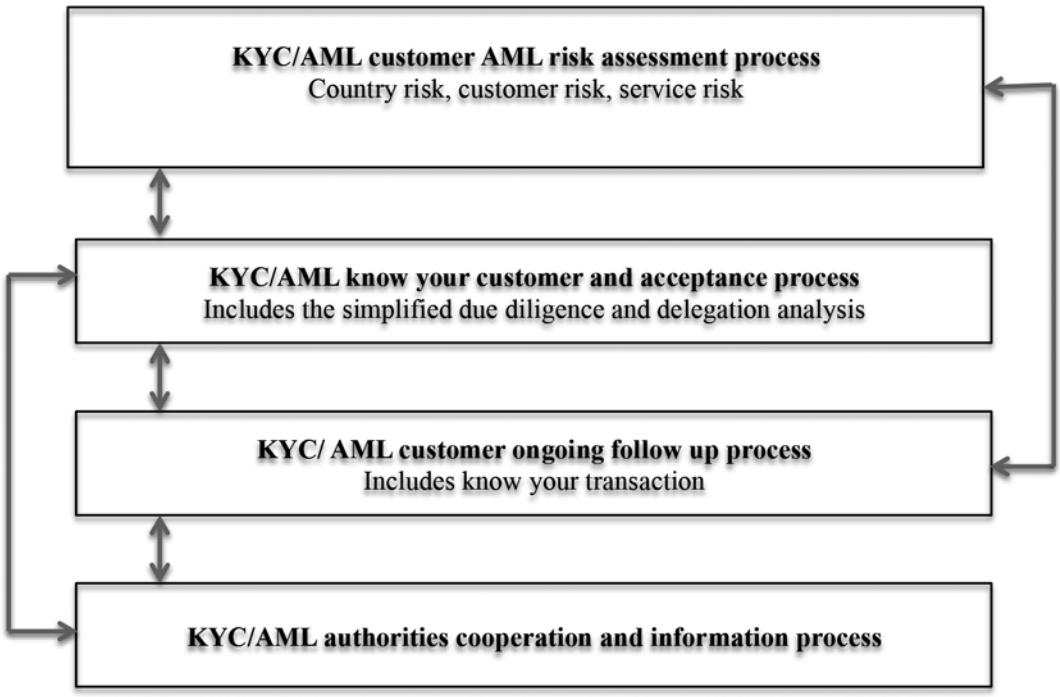
Alldridge (2008), stated that money laundering should be mitigated with international instruments which would make money laundering complicated and difficult. European Union has improved its anti-money laundering, policy with Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. Directive EU 2018/843 apply to the following obliged entities: (..) providers engaged in exchange services between virtual currencies and fiat currencies. This Directive also establishes: following definition applied: 'virtual currencies' means a digital representation of value that is:

- not issued or guaranteed by a central bank or a public authority;
- not necessarily attached to a legally established currency;
- not possess a legal status of currency or money;
- but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically;

At that time scientist were discussing, that "Policy makers hope that the risk-based approach will help reduce the number of poor quality reports and improve the quality of intelligence provided to FIUs. Nevertheless, the question of how to identify risks remains." (Gelemerova, 2009).

Banking KYC and AML process are presented in the table below. It is a four-level process which includes primary risk assessment of the customer, constant due diligence of the customer, then gathered information in the first stage is compared to the customer on-going transaction follow up. Is the customer in line with its declared activities, money origin, money turnover, etc. Finally due all stages of the operations information is shared with authorities if there are potentially risky transactions (Table 7).

Table 7. Private – Retail Banking KYC/AML standardized process



Source: Smet D.D., Mention A.L. (2011)

Subbotina (2009) determined that even Banks having strict requirements for AML and KYC procedures sometimes partially violates it. From the survey we can see that in all cases Bank has dedicated employees for AML procedures, however, breaches are related with the responsible employee that is responsible for AML and KYC compliance usually has other responsibilities, sometimes employees do not update information or report after the deadlines. The survey shows that even having strict regulation under the central bank and within the bank itself KYC and AML procedures are breaches or can be breached due to operational mistake.

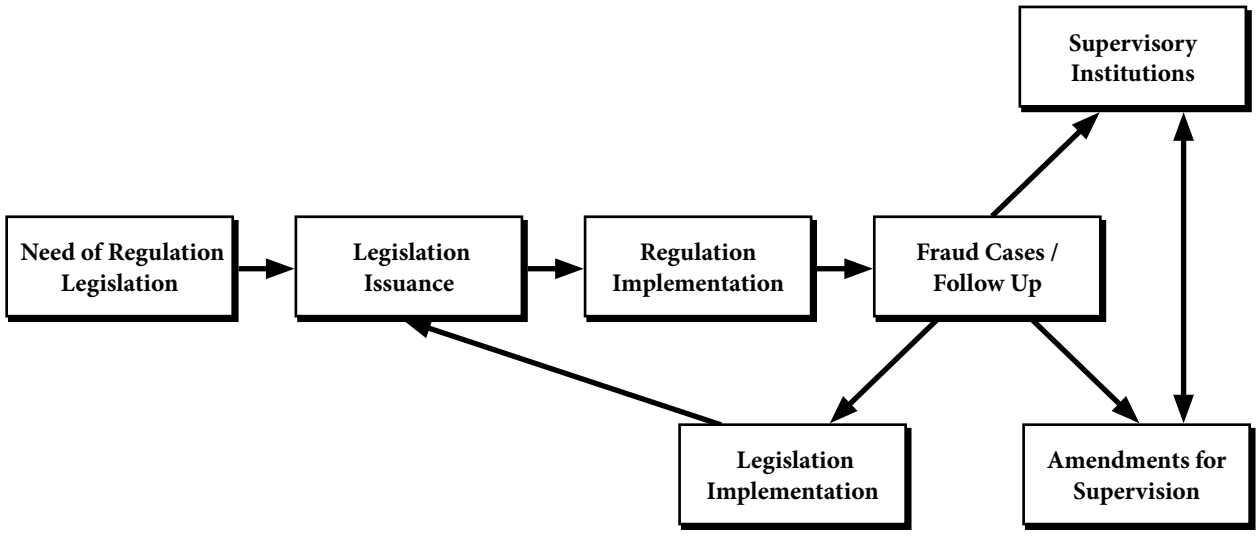
During the past few years, there was a row of money laundering cases in Banking sector: Danske Bank – 230 bln. USD (Bloomberg, 2019), Swedbank 10 bln. USD (Bloomberg, 2019), Nordea 405 mln. USD (Bloomberg, 2018), ABLV 102 mln. USD (The Baltic Course, 2018, Latvian Television, 2018). The money laundering cases were related to North Korea nuclear programme funding, money laundering by politicians and Russian citizens that are on the EU and USA sanction list. Unlike the Bitcoin Banks are listed in stock exchange, internal and external (BIG 4) auditors audit their financials, local authorities and ECB supervise them.

The outcome of Danske Bank independent auditors Brune & Hjejle (2018), is large scale money laundering case was caused by a) inadequate KYC procedure fulfilment b) inadequate AML procedure fulfilment c) lack or response of reporting personnel.

The tendency of KYC and AML implementation shows, that scientist hypothesis (Alldridge 2008, Gelemerova 2009, Subbotina 2009) regarding procedure implementation issues is confirmed by practical big scale money laundering cases, which are backed by institutional auditors Brune & Hjejle (2018) report.

The data of the money laundering cases should be used to make amendments in legislation of money laundering supervision. The fraud cases shows that the AML and KYC procedure implementation for Banks are still needed for improvements (Table 8).

Table 8. The process of Legislation issuance in financial sector and need of improvements



Source: made by authors

European commission has released 5th Money Laundering directive, which, will "limit the anonymity related to virtual currencies and wallet providers" (European Commission 2019). According European parliament decision (2018) it appears that there is background for risk mitigation implementation in Europe as KYC and AML procedures shall be implemented in custodian wallet providers and cryptocurrency – fiat currency exchanges. The Member States must transpose this Directive by 10 January 2020. Therefore it is expected that the risks related with KYC and AML procedures will be implemented in cryptocurrency market. European commission is considering that "These amendments introduce substantial improvement to better equip the Union to prevent the financial system from being used for money laundering and for funding terrorist activities."

Outstanding risks in cryptocurrency market shows, initial coin offering (hereinafter - ICO) cases. Ten biggest initial coin offerings from its release date caused at least 6.6 billion USD losses for its investors. The table shows that despite known companies, like Telegram or Petro cryptocurrency (supported by Venezuelian president Maduro), the results of biggest ICO revenues are very bad or not available. Value change in companies from the beginning of ICO (fund rise) up to the date of research 2019 07, shows that in all cases we see rapid decease in price (Table 9).

Table 9. Biggest ICO raised funds in Million USD and Value change from release up to date

	HDAC Technology	Telegram	Petro	TaTaTu	HDAC	Filecoin	Tezos	Sirin Labs	Bancor
Milion USD	6 580	1 700	735	575	258	257	232	158	153
Value change	-80%	n.a.	n.a.	-94%	-77%	-72%	-78%	-94%	-88%

Source: Bloomberg, 2018

However authors consider that cryptocurrency risk mitigations shall be observed in the near future as well as the KYC and AML implementation. As research showed that more likely implementation of KYC and AML implementation shall be challenging as Banking industry which is regulated by the same EU directive is still facing need for improvements.

Moreover cryptocurrency is a digital product and its KYC and AML implementation differs from other financial instruments therefore its would additionally face following challenges:

- It is unclear which institution will be able appropriately control procedure implementations;

- It is unclear weather competences of the supervision institution will be relevant for implementation of KYC and AML procedures for IT based financial tool (cryptocurrency – authors remark);
- Would it be efficient to implement KYC and AML procedures locally as cryptocurrency is aproduct of global economy, whereas risks and mitigations are homogenous for all countries?;
- Cryptocurrency transactions cannot be stopped due to its autonomy.

Conclusions:

- The research showed that regulaiton is neccesery for cryptocurrency market although legal regulation was not the aim of the reasearch. Authors emphsize that apropriate KYC and AML procedure implementation would have an impact on cryptocurrency risks integration.
- The KYC and AML procedures is necesery step to migitage risk carried by cryptocurrency.
- Banking case study of AML and KYC proceudres showed that despite of existing proceduresthere are still outstanding risks in procedure implementation and follow up, there fore it is important to execute further observation of KYC and AML procedure implementation execution.
- The reaserach showed that there might be obstacles to implement KYC and AML procedures as a) cryptocurrency is a product of global market b) there is no possibility to stop Bitcoin transaction de to its autonomity c) cryptocurrency is a new for of financial product having IT based operating model, therefore the new competences shall be needed to implement apropriate KYC and AML regulations.

References

Alldridge, P. (2008). Money laundering and globalization, *Journal of Law & Society*, 35(4): 437-463.

Alfa.lt (2018). FNTT paviešino kriptovaliutų rinkos apyvartą Lietuvoje, available at: https://www.alfa.lt/straipsnis/50331274/fntt-paviesino-kriptovaliutu-rinkos-apyvarta-lietuvoje

Asongu S., Boateng A., (2018), Introduction to Special Issue: Mobile Technologies and Inclusive Development in Africa, available at: https://doi.org/10.1080/15228916.2018.1481307

Asongu, S. A., & Nwachukwu, J. C. (2018). Comparative human development thresholds for absolute and relative pro-poor mobile banking in developing countries. *Information Technology & People*, 31(1): 63–93.

Barone, R., Masciandaro, D. (2019). Cryptocurrency or usury? Crime and alternative money laundering techniques, *European Journal of Law and Economics*, 47(2): 233-254, available at: https://doi.org/10.1007/s10657-019-09609-6

Bloomberg Businessweek. (2018). How's That ICO Working Out? Breaking down the biggest ICOs from the past few years, available at: https://www.bloomberg.com/news/articles/2018-12-14/crypto-s-15-biggest-icos-by-the-numbers

Bruun, Hjejle, (2018). Report on the Non-Resident Portfolio at Danske Bank's Estonian branch, available at: https://danskebank.com/-/media/danske-bank-com/file-cloud/2018/9/report-on-the-non-resident-portfolio-at-danske-banks-estonian-branch-.-la=en.pdf

Desmond D., Lacey D., Salmon P.M. (2019). Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. *Journal of Money Laundering Control*, 22(3): 480-497, available at: http://dx.doi.org/10.1108/JMLC-10-2018-0063

Cainmarketcap.com. (2019). All Crypto currencies, available at: https://coinmarketcap.com/all/views/all/

Clayton, J. (2018). Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC, available at: https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission#_ftn11

Cohen, L., Manion, L. (1989). Research Methods in Education, (3). London, England, ISBN 9780415044103

Crouch M., McKenzie H. (2006). The logic of small samples in interview-based qualitative research, *Social Science Information*, 45(4), available at: https://doi.org/10.1177/0539018406069584

Danton, B. (2014). Bitcoin and money laundering: Mining for an effective solution. *Indiana Law Journal*, 89(1): 441–472.

European Commission. (2019). Communication, Anti-money laundering and counter terrorist financing, available at: https://ec.europa.

eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en

EU Observer. (2019). Smurfing: How Russians laundered €4m in Belgium, available at: https://euobserver.com/justice/145370

Gelemerova, L. (2009). On the frontline against money-laundering: the regulatory minefield, *Crime Law Soc Change*, (52): 33–55, available at: https://link.springer.com/content/pdf/10.1007%2Fs10611-008-9175-8.pdf

European Parliament. (2015). Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, available at: https://publications.europa.eu/en/publication-detail/-/publication/0bff31ef-0b49-11e5-8817-01aa75ed71a1/language-en

European Parliament. (2018). DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=LT

Kordík, M., Kurilovská, L. 2017. Protection of the national financial system from the money laundering and terrorism financing, *Entrepreneurship and Sustainability Issues* 5(2): 243-262. http://doi.org/10.9770/jesi.2017.5.2(7)

Kvale, S. (1996). Interviews: An Introduction to Qualitative Research Interviewing, P. 145, 147, ISBN-10: 080395820X

Libby, R., Blashfield, R. (1978). Performance of a composite as a function of a number of judges. *Organizational Behavior and Human Performance*, (21): 121-129, available at: https://doi.org/10.1016/0030-5073(78)90044-2

Limba, T., Stankevičius A., Andrulevičius, A. (2019a). Industry 4.0 and national security: the phenomenon of disruptive technology, *Entrepreneurship and Sustainability Issues,* 6(3): 1528-1535. https://doi.org/10.9770/jesi.2019.6.3(33)

Limba, T., Stankevičius, A., Andrulevičius, A. (2019b). Cryptocurrency as Disruptive technology: Theoretical Insights. *Entrepreneurship and Sustainability Issues,* 6(4): 2068-2080. http://doi.org/10.9770/jesi.2019.6.4(36)

Lithuanian Bank. (2017). Lietuvos bankas skelbia poziciją dėl virtualiųjų valiutų, [Bank of Lithuania announces position on virtual currencies] available at: https://www.lb.lt/lt/naujienos/lietuvos-bankas-skelbia-pozicija-del-virtualiuju-valiutu

Mugarura N. (2014). Customer due diligence (CDD) mandate and the propensity of its application as a global, AML paradigm, *Journal of Money Laundering Control*, 17(1): 76-95, available at: https://doi.org/10.1108/JMLC-07-2013-0024

Murphy, J. T., & Carmody, P. (2015). Africa's information revolution: Technical regimes and production networks in South Africa and Tanzania, RGS-IBG book series. Chichester, UK: Wiley,

Tkachenko, V., Kwilinski, A., Korystin, O., Svyrydiuk, N. (2019). Assessment of information technologies influence on financial security of economy. *Journal of Security and Sustainability Issues*, 8(3): 375-385, available at: http://doi.org/10.9770/jssi.2019.8.3(7)

Tu, K. V.; Meredith, M. W. (2015). Rethinking virtual currency regulation in the bitcoin age. *Washington Law Review*, 90(1): 271-348.

Tvaronavičienė, M. 2018a. Elaborating internationally tuned approach towards critical infrastructure protection. *Journal of Security and Sustainability Issues,* 8(2), 143–150. https://doi.org/10.9770/jssi.2018.8.2(2)

Tvaronavičienė, M. 2018b. Towards efficient policy making: forecasts of vulnerability to external global threats. *Journal of Security and Sustainability Issues,* 7(3): 591–600. http://doi.org/10.9770/jssi.2018.7.3(18)

Remeikienė, R., Gasparienė, L., Schneider F.G. (2018). The Definition of Digital Shadow Economy. *Technological and Economic Development of Economy*, 24(2): 696–717, https://doi.org/10.3846/20294913.2016.1266530

Smet D.D, Mention A.L. (2011). Improving auditor effectiveness in assessing KYC/AML practices: Case study in a Luxembourgish context. *Managerial Auditing Journal* https://www.emeraldinsight.com/doi/pdfplus/10.1108/02686901111095038

Stankevičius, A., Lukšaitė, A. (2016). Transparent lobbying for sustainability: case of Lithuania. *Entrepreneurship and Sustainability Issues*, 4(2): 220-227. http://dx.doi.org/10.9770/jesi.2016.4.2(9)

Stankevičius, A., Kapranova L., Simanavičienė Ž., Lukšaitė A. (2016). Tax morale and tax evasion: theoretical insights, *Visuomenės saugumas ir viešoji tvarka* (16), PP. 80, https://repository.mruni.eu/handle/007/15020

Subbotina, N. (2009). Challenges that Russian banks face implementing the AML regulations, *Journal of Money Laundering Control*,

12(1): 19-32, https://doi.org/10.1108/13685200910922624

Swiss Association for Standardization. (2019). Current currency & funds code list, available at: https://www.currency-iso.org/en/home/tables/table-a1.html

Šimonová, J,, Čentéš, J., Beleš, A. 2019. Financial analysis of innovative forms of money, *Entrepreneurship and Sustainability Issues* 7(1): 69-80. http://doi.org/10.9770/jesi.2019.7.1(6)

Štitilis, D., Pakutinskas, P., Malinauskaitė, I. (2016). Preconditions of sustainable ecosystem: cyber security policy and strategies. *Entrepreneurship and Sustainability Issues* 4(2): 174-182. https://doi.org/10.9770/jesi.2016.4.2(5)

The Economist. (2019). By The Same Token, The Weapons of Mass Disruption, June 8th – 14th 2019, p.9.

The Guardian. (2019). Libra: Facebook launches cryptocurrency in bid to shake up global finance, available at: https://www.theguardian.com/technology/2019/jun/18/libra-facebook-cryptocurrency-new-digital-money-transactions

The President of the United States. (2017). National Security Strategy of the United States of America, available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Tidikis, R. (2003). Socialinių mokslų tyrimų metodologija. P. 357, Vilnius: Lietuvos teisės universiteto leidybos centras, 2003, ISBN9955-563-26-5, available at: https://www.scribd.com/doc/36462514/Tidikis-Socialiniu-Moksliniu-Tyrimu-Metodologija

Wamboldt, B.D. (1992). Content analysis: Method, applications, and issues, *Health Care for Women International* (13): 313-321, available at: https://doi.org/10.1080/07399339209516006

Zetzsche, D. A., Buckley, R. P., Arner, D. W. (2018). The distributed liability of distributed ledgers: Legal risks of blockchain. University of Illinois Law Review,2018(4): 1361-1406, available at: https://heinonline.org/HOL/Page?handle=hein.journals/unilllr2018&div=41&g_sent=1&casa_token=XokbCrxchQAAAAAA:lpEjFAuilxS6qnJd4i23FNv9dzR7fsJoNiPnBcuXN_TP-6DqeUVGiBuy76yQ2DzKqbP-huFC&collection=journals

Tadas LIMBA is associate professor at Mykolas Romeris University (email: tlimba@mruni.eu). He obtained a PhD degree in Management from Mykolas Romeris University in 2009. He is the head of Joint Study Programs "Informatics and Digital Contents" with Dongseo University in South Korea, which is taught in English at Mykolas Romeris University. His research interests include over than 15 Years of experience in the fields of E-Government, E-Business, IT application for the organizational change and Digital Contents. He is actively developing and expanding the relations for the future prospective of the common activities with Dongseo University. Tadas Limba has over 30 scientific publications on different topics related with New Public Management, E-Government, E-Signature, E-Time Stamping, E-Business, E-Marketing, IT and Patent Law, Biotechnology Strategies. He is also an international expert in the field of E-Government and trained faculty members of the Public Administration Academy of the Republic of Armenia and Eurasian International University in Armenia in 2014. Tadas Limba visited Communication University of China in 2014 and had research internships at Arizona State University, USA and at Dongseo University, South Korea in 2015.
ORCID ID: orcid.org/0000-0003-2330-8684

Andrius STANKEVIČIUS, Mykolas Romeris University, Faculty of Public security, Department of Law, lector. Research interests: public security, interest groups, lobbying.
ORCID ID: orcid.org/0000-0002-2528-0497

Antanas ANDRULEVIČIUS, JSC "Financial Figures", consultant. Research interests: disruptive technologies, crypto currency, national security, Industry 4.0.
ORCID ID: orcid.org/0000-0002-5531-5267

Register for an ORCID ID:
https://orcid.org/register