TERRORIST FINANCING, VIRTUAL CURRENCIES, AND THE FUTURE OF SECURITY

Mina ZIROJEVIĆ [*]
Darko M. MARKOVIĆ [**]

Abstract

Perceived risk in terrorist use and widespread adoption of virtual currencies over the past few years has driven the notion that this innovation represents a serious threat to security. This article addresses this issue, examining the security implications associated with the rise of this technology. In this article we will first try to present an overview of this question to subsequently sketch out a theoretical framework based on a critical approach to security. The article then considers patterns and methods of terrorist financing to help situate virtual currencies in this context, arguing that some of the alleged benefits offered by this technology are limited. In consequently considering the case of ISIL, it determines that the organization's current financing needs are best served by their established methods and not virtual currencies. The final section then returns to the question of security, showing that a number of practices have resulted in the gradual securitization of this technology, and advocating for its de-securitization, or its negotiation in the political realm and not one defined by the logic of emergency.

Key Words*: bitcoin, cybercrime, security, terrorism, terrorist financing*
JEL Classification: [K24]

1. Introduction

New innovative technologies that enable digital transactions and the delivery of financial products and services in new online networks, environments and marketplaces are virtual currencies (VCs). Virtual currencies include cryptocurrencies such as Bitcoin, as well as a range of other digital value-transfer methods.

As all other innovations, especially in the financial area, we can observe positive sides of virtual currencies as important for furthering competition in payments services, expanding financial inclusion and enabling greater efficiency and speed in cross-border value transfer. On the other side, however, virtual currencies have features that present risks for facilitating criminality, including money laundering and terrorist financing. The borderless nature and anonymity of virtual currencies allows terrorist actors to transfer funds outside the regulated sector and beyond the purview of anti-money laundering and countering the financing of terrorism (AML/CFT) authorities. Instances of virtual currencies' illicit use in cybercrime and in encrypted Dark Web marketplaces have been well documented.

[*] Associate Professor/Research Assistant, Ph.D., Institute of comparative Law, Belgrade, Serbia.
[**] Assistant professor at Faculty of European Legal and Political Studies, University Business Academy, Novi Sad.

However, there are still only a small number of publicly documented and confirmed cases of terrorist financing involving virtual currencies. For now, we cannot see the full scope of using Virtual Currencies for terrorism purposes, but it is certainly time to tackle this notion before it is too late.

In the near-term future, terrorist use of VCs is most likely to involve occasional use for specific and limited purposes, including:[1]

- raising funds or procuring illicit items on the Dark Web;
- soliciting donations in crowdfunding campaigns conducted on social media and encrypted messaging platforms; and
- transmitting funds internationally among members of terrorist networks using P2P value transfers.

This article addresses this issue, examining the security implications associated with the rise of this technology. It this article we will first try to present an overview of this question to subsequently sketch out a theoretical framework based on a critical approach to security. It then considers patterns and methods of terrorist financing to help situate virtual currencies in this context, arguing that some of the alleged benefits offered by this technology are limited. In consequently considering the case of ISIL, it determines that the organization's current financing needs are best served by their established methods and not virtual currencies. The final section then returns to the question of security, showing that a number of practices have resulted in the gradual securitization of this technology, and advocating for its de-securitization, or its negotiation in the political realm and not one defined by the logic of emergency.

2. Problem of definition

Bitcoin is generating tremendous attention worldwide. On April 14, 2020, a Google search found 605 million results for Bitcoin. The most searched Bitcoin-related topics include bitcoin as a payment system, price, USD, Bitcoin network (software), and bitcoin value.

Nevertheless, there is no single global definition of the term 'virtual currency'. Indeed, the French and German finance ministries have suggested that the use of the term 'currency' when describing these technologies is misleading and that a new term, such as 'crypto-assets', may prove appropriate. (Letter from France and Germany to the G20 Ministers, 7 February 2018:1).

However, to provide for a common regulatory approach, the EU has adopted a definition of virtual currencies derived from the Financial Action Task Force's (FATF) guidance. EU observes virtual currencies as 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of

[1] Directorate General for Internal Policies, 2018, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, Study for the TERR Committee, PE 604.970-May 2018.

exchange and which can be transferred, stored and traded electronically.' In its 2014 report of Virtual Currencies: Key Definitions and Potential AML/CFT risks (Financial Action Task Force 2014:5), the Financial Action Task Force defined two forms of virtual currencies: decentralised virtual currencies and centralised virtual currencies.

In terms of value, scholars and practitioners have considered bitcoin to be a currency, using several terms to specify the type of currency. In the literature we can read different ideas for determination (Sinha, 2014): cryptographic (Morisse & Ingram 2016:5), virtual (Ram, Maroun, and Garnett 2016:2), digital (Plassaras 2013:379), private (Plassaras 2013:379), online (Lambert 2015:91), or electronic (Park & Park 2017:1). Of course, some researchers took money or a form of money as a basis for clarification (Lambert 2015:91:88), including digital money (Lambert 2015:88), a money-like informational commodity (Sinha 2014), a unit of value (Piotrowska 2016), a unit of account (Plassaras 2013), or a medium of exchange (Tu & Meredith 2015).

Although a virtual currency does not fulfil the basic functions of money, so it cannot be considered money, there are scholars and practitioners describing it as a software application or technology primarily linked with money. For them (Jacobs, 2011), Bitcoin is a system associated with financial operations (Rose 2015), online monetary transactions (Lambert 2015), e-transaction (Vassiliadis et al. 2017), financial control (Richter, Kraus, and Bouncken 2015), e-payment (Ryan 2017), and electronic cash (Jacobs 2011). Others try to link Bitcoin just to computer networks, as a peer-to-peer (Simser 2015) consensus (Lambert 2015) payment network (Abramowicz 2016), or an open-source software platform (Jacobs 2011) and an online communication protocol (Böhme et al. 2015) that uses blockchain technology (Jin Ho and Jong Hyuk 2017).

If we look on those definitions very carefully, we can find six main fundamental aspects that characterize this currency or technology: decentralized (Piotrowska 2016); irreversible (Simser 2015); pseudonymous (Bryans 2014); unregulated (Plassaras 2013); cheap (Morisse and Ingram 2016); and trusted (Morisse and Ingram 2016). Furthermore, if we read the first letters of each of these six characteristics of bitcoin, we can find the acronym DIPUCT.

If we consider Bitcoin both as a unit of value and technology, we will come to the same solution as the other authors: Bitcoin is a computer-based currency with no physical legal counterpart, used as a medium of exchange through an open system of computer networks and online communication protocols (Wamba et al, 2018: 11).

Virtual currencies are not used to compare relative prices between different goods and services, so their use is still limited to a small number of cases. No public authority issues virtual currencies. Therefore, they cannot be a means of saving either. The logical question is, why are they used then? The answer lies in the fact that their investors are motivated by fast earnings, on a huge scale, and this can be considered a speculative business. It all takes place on virtual currency exchanges, and all earnings are placed in the so-called digital wallets. The number of different virtual currencies is not limited, which is why there are more and more different

currencies in that market. However, there are limitations in terms of their offer, and they are reflected in very complicated and sophisticated technical solutions and processes that are not easily understood by the general public.

3. Bitcoin abuse for terrorism purposes

The evolving technology can be a blessing and a curse, depending on its use. New threats caused by evolving technology and older threats are observed to threaten the individuals and societies while the conventional threats continue to exist. For instance, the al-Qaeda terrorist organization converted passenger airplanes, which facilitate the life of humanity, into conventional missiles that resulted in death and injury to thousands of people.

Information Technologies brought about advancements that contributed most to the development of individuals and societies. These positive developments have been adapted by terrorist organizations into their activities. Terrorist organizations utilized the cyberspace, which emerged as the result of the developments in the IT field, for their activities, which gave rise to the invention of the notions of cyber terrorism or cyber-attacks. On the other side, it is obvious that an environment in which such a wide range of illegal services are offered appeals to the terrorist organizations. In this notion, we have sales of drugs and weapons by Bitcoin, money laundering, illegal pharmaceutical sales, and fake passports sales on the dark web, blackmailing through ransomware virus via the TOR network called the 'dark web'.

Virtual currencies-enabled cyber criminality may offer an attractive method for other actors seeking both to raise funds and cause disruption. In theory, it seems logical that this would be attractive to terrorist groups such as ISIS and al-Qaeda. With its 'flagship strategic report on key findings and emerging threats and developments in cybercrime - threats that impact governments, businesses, and citizens in the EU' (IOCTA n.d.), the Europol informs the public about these contemporary security risks every year. In the 2017 IOCTA Report, Europol suggests that, whilst terrorists make use of the internet and online communication apps for coordination, propaganda, and knowledge dissemination, their ability to launch cyber-attacks remains limited (Europol 2017:13).

According to the European Parliament, terrorist organizations utilize the cryptocurrencies for direct donations or fundraising through criminal activities, money transfer by converting into cash the money transferred to regions near conflict areas and funding activities to be conducted by organization members or travels (Directorate General For Internal Policies 2018:23).

However, the notion of 'cyber-jihad' is becoming more common and describes a situation where the cyber-world is fundamental to terrorist operations today. For example, ISIS poses an 'active cyber threat by working with lone hackers, hacker groups and by appropriating open-source online materials' (Ashok 2016). The case of Kosovo national Ardit Ferizi (known in the media as the 'Albanian Hacker') is one such example of the convergence of cybercrime, terrorism and VCs, and provides a suggestion of what the future may hold. In

August 2015, Ferizi installed malware to obtain personal information of the US government and military workers that was then published by ISIS as a 'hit-list' (Associated Press, 24 September 2016). He then demanded a ransom in Bitcoin from the company to remove the malware (Johnson 2016). Although Ferizi failed to obtain any Bitcoin, the crime demonstrated a terrorist actor's capability to engage in hacking and obtain confidential information.

A virtual currency might appeal to a terrorist organization aspiring to achieve financial self-sufficiency. ISIS demonstrated its general desire for financial self-sufficiency in 2015 when it announced the creation of the gold dinar, a physical currency it claimed to have created, in its own words, to avoid 'America's capitalist financial system of enslaver' (Staufenberg 2015). Whilst it failed to supplant the US dollar in ISIS's own operations, the launch of the gold dinar represents terrorist groups' aspirations for financial independence. By trading oil from 34,000 square miles of oil fields under its control, ISIS conducted an economic experiment, trying to replace American, Syrian and Iraqi money with the so-called gold dinar. The origin of this idea is historical, on the example of Abd al-Malik ibn Marwan, the leader of the Islamic empire from the Middle Ages, the Umayyad Caliphate, who ordered the creation of new coins intended to economically connect Muslims from all over the world. The goal of ISIS was not to unite the Muslim world in that way, but to destabilize the American economy by striking at the petrol-dollar system, considering that that system is the American "Achilles' heel" – it was a kind of extension of the 2001 attack on the World Trade Center, aimed at destroying the global economy. (O'Leary 2019). At the end of 2014, ISIS officially introduced the new currency, announcing the launch of a series of seven coins "divided between two gold dinars, three silver dirhams and two copper fulûs" (Moos 2018). ISIS earned about 60 million dollars a month from the controlled sale of oil, contributing to the strengthening of the American dollar, so the gold dinar was first introduced in the oil sector. Oil could only be bought for that fictional currency, so buyers had to buy a gold dinar beforehand. Soon (at the end of 2015), the gold dinar became a mandatory currency on the territory controlled by ISIS, and when oil sales reached a daily level of 150 thousand barrels, thanks to the price difference per gram of gold, one gold dinar was worth 30 US dollars (O'Leary 2019).

Initial Coin Offerings (ICOs) are another innovation that warrant mention in this context. ICOs are predominately associated with start-up ventures, but they have proven controversial and putatively high-risk. Fraudsters have used the uneven regulatory environment around ICOs to exploit often uneducated and unprotected victims.[2] Given their fundraising potential, it is perhaps unlikely, but certainly not

[2] In early 2018, the US Securities and Exchange Commission brought charges against Centra Tech Inc. for fraudulently promoting an ICO that raised USD 32 million (Peterson, Becky, 'The SEC charges a third Centra cryptocurrency "mastermind" with fraud over its $32 million ICO,' Business Insider, 20 April 2018, http://uk.businessinsider.com/sec-charges-third-centra-crypto-founder-withfraud-2018-4). In November 2017, a purported cryptocurrency company operating by the name Confido raised USD 375,000 through an ICO, only to disappear with the funds of duped investors

impossible, that terrorist actors could seek to raise funds under the guise of an ICO they have launched, either overtly or fraudulently.

This deviation from the classic form of virtual currency has basis in Islam that prohibits speculation, so it would be difficult to expect Muslims to use such a currency. Therefore, this is not about the Islamic interpretation of the parameters that determine money, but about unacceptable behaviour that virtual currency causes. When it comes to moral (religious) unacceptability of virtual currency for the Islamic world, it can have advantages for terrorist activities. Namely, in order to avoid legal and financial risks from aiding terrorist organizations, cryptocurrency can be a very suitable tool for anonymous assistance to terrorism. Anonymity plays a very important role in terrorist activities but is even more important for those who provide material support to terrorist organizations. (Petrović 2018: 51)

4. Problems and risks of cryptocurrency

The very fact that virtual currencies are not issued by central banks, nor backed by public authorities, speaks to the security shortcomings of their use. The very essence of cryptocurrency business is in the possibility of quickly making a large profit, and it has a dark side - in such transactions, someone has to suffer a large loss. This is especially true if we keep in mind that payment transactions in virtual currencies take place outside the official payment systems. It makes such transactions unsafe because, unlike in regular money transactions, there is no investment insurance here. The purchase and exchange of virtual currencies take place on special platforms, where it is possible to purchase virtual currencies with real money and exchange one virtual currency for another. If such a platform is compromised, large losses of assets in virtual currencies can occur.

Insufficient knowledge about the technological processes the use of cryptocurrencies is based on blurs the background value of virtual currencies. Unlike electronic money, which is always paid out at face value, due to sudden price changes, the value of cryptocurrency payment is not equal to the previously invested monetary value. Therefore, investing in cryptocurrencies is very risky. This risk increases day by day, along with the rapid development of a huge number of virtual currency networks. There is also an increasing risk of exposure to theft or data loss. In addition to that, such a number of networks enables large oscillations in the value of virtual currencies as well as to be compromised. The value of cryptocurrency is unpredictable, subject to drastic changes, and even the slightest inadvertence could be cardinal for an investor.

The anonymity of these transactions makes it difficult to detect them, so they are suitable for transactions related to various crimes. It is why the use of cryptocurrencies for money laundering and terrorist financing poses a special challenge in the fight against organized crime and terrorism. The cryptocurrency

(Kharpal, Arjun, 'Cryptocurrency start-up Confido disappears with $375,000 from an ICO, and nobody can find the founders,' CNBC, 21 November 2017, https://www.cnbc.com/2017/11/21/confido-ico-exit-scam-founders-runaway-with-375k.html.).

transactions themselves are publicly available, but user's identification is not permanent – it is linked to the address of the virtual wallet, which gives a new cryptocurrency address with each new transaction, so it is difficult to track the real user. Today, there are developed companies that deal with exchange transactions in virtual currencies, but despite the high standards they warrant, there are no definite guarantees to prevent their abuse for terrorism. This is particularly pronounced in countries where large transactions are allowed without control, meaning, without international cooperation, which is extremely important in combating money laundering and terrorist financing.

This kind of business is becoming more internationalized, and today there are more and more servers (mines) where virtual currencies are mined – the servers and the companies working in this business are registered in one country, while the business is done abroad. Under such circumstances, there is the problem of criminal prosecution, because virtual currencies are banned in some countries, while in others they are considered a regular financial instrument (Stajić, Mirković & Radivojević 2018: 903). Due to local jurisdiction, 'taking measures to detect, prosecute, and conduct criminal proceedings for acts of high-tech crime is limited to the territory of the state' (Pisarić 2013: 293). This is certainly a great reason for the international community to better organize itself and establish unified control over these transactions. Due to the immense damage that can occur from the use of virtual currency exchanges for money laundering and terrorist financing, such organization of the international community should be able to encompass countries that are known as tax havens, as well.

Conclusions

Although cryptocurrencies have been developed for different purposes, the lack of a control mechanisms due to the challenges in detecting users and obtaining traffic data makes the utilization of them by trans-border criminals appealing.

Intersection of cyber criminality and terrorism could prove to be a new frontier in terrorist capabilities and could provide considerable terrorist financing opportunity should it ever accelerate on a large scale. It therefore requires greater understanding and law enforcement engagement to ensure it is effectively monitored and countered over time should it emerge.

Several developments could elevate and shape the nature of these risks over time, especially: the proliferation of virtual currencies featuring high levels of privacy and anonymity; terrorists' broader adoption and utilization of encryption technology, social media and other online platforms; the nexus between terrorist actors and other criminal activity; and the general pace and shape of virtual currencies innovation and adoption in a broader sense.

The underlying reasons for organizations to incline towards the 'dark web' and utilization of crypto currencies are to obfuscate the identities of their members and sympathizers, to carry on the propaganda activities and to be able to continue obtaining finances. It is envisioned that the current utilization is going to spread out

in inverse correlation to loss of territories and that other organizations, following the ideology of al-Qaeda, are going to increase their activities in the cyber space over time.

The prospect for sustained, larger-scale terrorist financing to emerge through developments such as the convergence of terrorism with cyber criminality presents a possible long-term risk of concern. The EU regards mitigating the terrorist financing risks associated with virtual currencies as a significant security priority. The EU's recently adopted Fifth Anti-Money Laundering Directive (5AMLD) requires that Member States bring Virtual Currencies (Staufenberg 2015) exchange platforms and custodial wallet providers. To ensure its effectiveness, Member States should clarify the scope and purpose of regulation once transposed locally and must undertake meaningful enforcement.

It is obviously impossible that the countries, or even the EU can solitarily implement the precautions taken in cyber space. It is considered necessary to make decisions regarding legal amendments on enforcing international cooperation, operating secret investigations within the bodies of INTERPOL and Europol, providing multinational virtual patrol services, making overseen deliveries in-between states, registering the crypto-currency manufacturers and cryptocurrency miners in the scope of the UN.

Cooperation between governments and international organizations is compulsory to fight against cyber terrorism effectively because cyber terrorism is a multi-discipline matter like other computer-related crimes. User awareness, which is the most important element in the information security concept, especially in order to reach the sufficient level of awareness in cryptocurrency users, trainings, conferences, seminars and social responsibility projects should be organized in the medium and long term.

Bibliography

1. Abramowicz, M., 2016, 'Cryptocurrency-based law', *Arizona Law Review*, 58(2), pp. 359-420.
2. Ashok, I., 2016, 'The anatomy of a "Cyber Jihad" – analyzing the future and evolution of terrorism in cyberspace', *International Business Times*, 20 June, viewed 20 March 2020, from ttps://www.ibtimes.co.uk/anatomy-cyber-jihad-analysing-evolutionfuture-terrorism-cyberspace-1566184.
3. Associated Press (AP), 2016, 'Hacker who gave ISIS "hitlist" of US targets jailed for 20 years', The Guardian, 24 September, viewed 22 March 2020, from https://www.theguardian.com/world/2016/sep/24/hacker-who-gave-isis-hitlist-of-us-targets-jailed -for-20-years.
4. Böhme, R., Nicholas, C., Edelman, B. & Moore, T., 2015, 'Bitcoin: Economics, Technology, and Governance', *The Journal of Economic Perspectives*, 29(2), pp. 213-238. doi: http://dx.doi.org/10.1257/jep.29.2.213.

5. Bryans, D., 2014, 'Bitcoin and Money Laundering: Mining for an Effective Solution', *Indiana Law Journal*, Vol. 89, (1), pp. 441-472. Available at: http://www.repository.law.indiana.edu/ilj/vol89/iss1/13.
6. Directorate General For Internal Policies, 2018, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, Study for the TERR Committee, PE 604.970-May 2018, European Parliament's Policy Department For Citizens' Rights And Constitutional Affairs, viewed 24 March 2020, from https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOLSTU(2018)604970_EN.pdf
7. European Parliament, 2018, *Prevention of the use of the financial system for the purposes of money laundering or terrorist financing*, P8_TA(2018)0178, Position of the European Parliament adopted at first reading on 19 April 2018 with a view to the adoption of Directive (EU) …/… of the European Parliament and of the Council 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, Article 3 new point 18 of the Directive (EU) 2015/849, viewed 20 March 2020, from https://www.europarl.europa.eu/doceo/document/TA-8-2018-0178_EN.pdf.
8. Internet Organised Crime Threat Assessment (IOCTA), n.d., [Online], viewed 21 March 2020 from https://www.europol.europa.eu/iocta-report.
9. Europol – European Cybercrime Centre, 2017, *Internet Organised Crime Threat Assessment (IOCTA) 2017*, viewed 21 March 2020, from https://www.europol.europa.eu/iocta/2017/THE_CONVERGENCE_OF_CYBER_AND_TERRORISM.html.
10. Financial Action Task Force, 2014, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks', Report, June, viewed 21 March from http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and -potential-amlcft-risks.pdf.
11. Jacobs, E., 2011, 'Bitcoin: A Bit Too Far?', *Journal of Internet Banking and Commerce* (Online), 16(2), 1-4, viewed 24 March 2020, from http://www.icommercecentral.com/open-access/bitcoin--a-bit-too-far-.php?aid=38265.
12. Johnson, T., 2016, 'Computer hack helped feed an Islamic State Death List', McClatchy, 20 July, viewed 22 March 2020, from http://www.mcclatchydc.com/news/nation-world/national/ article90782637.html.
13. Lambert, E. E., 2015, 'The internal revenue service and bitcoin: A taxing relationship', *Virginia Tax Review*, Vol. 35.1, 88-115.
14. Letter from France and Germany to the G20 Ministers, 7 February 2018, https://www.politico.eu/wp-content/uploads/2018/02/G20-Letter-on-crypto-assets-tokens.pdf.
15. Moos, O., 2018 December 23, 'The Return of the Gold Dinar – An analysis of the Islamic State coin production', *Religioscope,* viewed 22 March 2020 from https://english.religion.info/2018/12/23/ the-return-of-the-gold-dinar-an-analysis-of-the-islamic-state-coin-production/.
16. Morisse, M. & Ingram, C., 2016, 'A mixed blessing: Resilience in the entrepreneurial sociotechnical system of bitcoin', *JISTEM - Journal of Information Systems and Technology Management*, 13(1), pp. 3-26, doi: http://dx.doi.org/10.4301/S1807-17752016000100001.
17. O'Leary, RR, 2019, 'Sharia Goldbugs: How ISIS Created a Currency for World Domination', viewed 22 March 2020 from https://www.coindesk.com/sharia-goldbugs-how-isis-created-a-currency-for-world-domination.

18. Papadopoulos, P., Vassiliadis, S., Rangoussi, M., Konieczny, T. & Gralewski, J., 2017, 'Bitcoin value analysis based on cross-correlations', *Journal of Internet Banking and Commerce* 22 (S7), pp. 1-12, viewed 24 March 2020, from https://www.researchgate.net/publication/323993232_BITCOIN_VALUE_ANALYSIS_BASED_ON_CROSS-CORRELATIONS.
19. Park, J.H. & Park J.H., 2017, 'Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions', *Symmetry (20738994)* 9 (8), 1-13. doi: http://dx.doi.org/10.3390/sym9080164.
20. Petrović, R., 2018, 'Usages of Modern Technologies by Islamic Fundamentalists', *Nauka i društvo*, (8), pp. 40-54.
21. Piotrowska, A. I., 2016, 'Fields of potential use of cryptocurrencies in the payment services market in Poland-results of an empirical study', *Copernican Journal of Finance and Accounting* 5 (2), pp. 201-217.
22. Plassaras, N. A., 2013, 'Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF', *Chicago Journal of International Law*, 14(1), pp. 377-407.
23. Ram, A., Maroun, W. & Garnett, R., 2016, 'Accounting for the Bitcoin: accountability, neoliberalism and a correspondence analysis', *Meditari Accountancy Research*, 24(1), pp. 2-35.
24. Richter, C., Kraus, S. & Ricarda B. B., 2015, 'Virtual Currencies Like Bitcoin as a Paradigm Shift in the Field of Transactions', *International Business & Economics Research Journal*, 14(4), pp. 575-585. doi: http://dx.doi.org/10.19030/iber.v14i4.9350.
25. Rose, C., 2015, 'The Evolution of Digital Currencies: Bitcoin, a Cryptocurrency Causing a Monetary Revolution', *International Business & Economics Research Journal*, 14(4), 617-n/a. doi: http://dx.doi.org/10.19030/iber.v14i4.9353.
26. Ryan, P., 2017, 'Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain', *Technology Innovation Management Review*, 7(10), pp. 14-21. Doi: http://dx.doi.org/10.22215/timreview/1110.
27. Simser, J., 2015, 'Bitcoin and modern alchemy: In code we trust', *Journal of Financial Crime*, 22(2), pp. 156-169, doi:10.1108/JFC-11-2013-0067.
28. Sinha, A., 2014, 'Bitcoins: A Super Bubble Ready to Burst', *FIIB Business Review*, 3(3), pp. 3-6. doi: http://dx.doi.org/10.1177/2455265820140301.
29. Staufenberg, J., 2015, 'Isis shows off currency with gold dinar coin worth £91 each – in quest for "world domination"', Independent, 31 August, viewed 23 March 2020, from https://www.independent.co.uk/news/world/middle-east/isis-shows-off-newcurrency-with-gold-dinar-coins-worth-91-each-in-quest-for-world-domination-10480121.html.
30. Tu, K.V. & Meredith, M., 2015, 'Rethinking virtual currency regulation in the bitcoin age', *Washington Law Review*, Vol. 90 (1), pp. 271-347.
31. Wamba, S. F., 2018, 'Bitcoin, Blockchain, and FinTech: A Systematic Review and Case' Volume 31, 2020 - Issue 2-3. doi: htps://www.tandfonline.com/doi/full/10.1080/09537287.2019.1631460.