

JUDr. Michaela Jurisová, PhD.  
Academy of the Police Force in Bratislava  
Department of Criminology  
PhDr. Elena Nikolajová Kupferschmidtová, PhD.  
Academy of the Police Force in Bratislava  
Department of Languages

## Virtual Currencies versus Crime in the Context of the Slovak Republic

### Introduction

The primary focus of the present paper is laid on virtual currencies with the presentation of some risks related to the use of virtual currencies and the possibilities of detecting and clarifying the crime associated with them. The selected findings and their association with the most elaborate, i.e. the most popular virtual currency/system – bitcoin are presented.

For the purposes of the present paper the term "*virtual currency*" is used in the light of established practice, while respecting the fact that the European Central Bank does not regard virtual currencies, such as Bitcoin, as full forms of money as defined in economic literature. Virtual currency is also not money or currency from a legal perspective. The cryptocurrencies can undoubtedly be described as a phenomenon of recent years (especially in the world of finance). Virtual payments are experiencing a huge expansion, they are in the sights of many people and institutions. They are associated with both positives and negatives. Cryptocurrencies can be viewed from a multidisciplinary perspective.

From the methodological point of view, selected theoretical and empirical methods were used such as analysis and synthesis of facts from legal documents, scientific literature, and other relevant materials, prognostic method, or incorporation of knowledge resulting from the implementation practices (namely from interviews with experts on the subject matter).<sup>1</sup> In the selected passages, the authors pay particular attention to the Slovak setting of the subject matter.

Digitization and virtual reality form an integral part of the everyday life of all human beings. Nowadays, we all live, wittingly or unwittingly, in virtual reality and we are an integral part of it. We are gradually entering cyberspace and this world is being transmitted to all forms of real life. Just as we create a virtual personality on social networks, we have gradually created virtual currencies within business communication. And the tendency to create digital money has existed since the beginning of the expansion of the Internet.

Just as financial crimes occur in everyday life, they find their place in the virtual world, e. g. there is damage to personal identity and property, or a possibility to create space for trade in prohibited goods and services. Among others, an important research

---

<sup>1</sup> The interviews were conducted with the Cyber Crime Department Experts from the Office of Criminal Police of the Police Force Presidium.

question is to what extent virtual currencies, as the research matter, are abused in the territory of the Slovak Republic and what are the specific conditions that allow such abuse. In addition to research on legal and scientific literature, the authors sought answers in implementation practice.

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 (hereinafter referred to as 'Directive') as one of the core legal documents sets out an efficient and comprehensive legal framework for addressing the collection of money or property for terrorist purposes by requiring the Member States to identify, understand and mitigate the risks related to money laundering and terrorist financing and also partially refers to virtual currency pitfalls.<sup>1</sup>

## **The Main Objective**

At the same time, the attention should be drawn to the European Commission's Report (EC Report to the European Parliament on Risk Assessment of Money Laundering and Terrorist Financing, Brussels, 26 June 2017), which identified forty products or services of the highest vulnerability. The biggest risks are the use of cash, virtual currencies, crowdfunding, the financing of non-profit organizations or the provision of informal money transfer services, such as the *hawala* system.<sup>2</sup>

Selected features of cryptocurrencies allow their misuse for criminal purposes, such as terrorist financing or money laundering. Thus, their use for illegal purposes is obvious. But there are also a number of positives associated with cryptocurrencies.

Given the fact that the number of virtual currency scheme(s) (hereinafter referred to as 'VCS') is constantly changing, the focus was on those VCS which consistently ranked among the top ten positions as regards market capitalization in August 2020: Tether, Bitcoin, Ethereum, Litecoin, EOS, XRP, Bitcoin Cash, Chainlink, Bitcoin SV, OMG Network.<sup>3</sup> Virtual currencies are considered still as a new phenomenon that is rapidly changing on everyday basis. As the rapid changes of virtual currencies can not be grasped properly, the obvious indication of risks comes to light.

The ever-increasing digitization affects the financial sphere thus the focus is transitioning towards this form. As virtual cryptocurrencies are increasingly penetrating the lives of the general public, the interest from the states perspective in cryptocurrencies is continually increasing. Thus, the need to expand and combine the

---

<sup>1</sup> The European Central Bank avoids the term "virtual currency" or "cryptocurrency" and the term "virtual currency scheme(s)" (VCS) is used instead as virtual currencies such as Bitcoin can not be regarded as full forms of money as defined in economic literature. However, it is defined as a digital representation of value, which in some circumstances can be used as an alternative to money. For more information see ŠIŠULÁK, S. et L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti*, p. 274.

<sup>2</sup> See SABAYOVÁ, M. et M. PRESPERÍNOVÁ, 2018. *Vybrané riziká prania špinavých peňazí*, p. 124 and following.

<sup>3</sup> The current status of the range of decentralized VCS can be found at <http://coinmarketcap.com/all.html>.

knowledge about the cryptocurrencies is of vital importance as they bring not only the benefits and they also pose a threat to societies around the world.

The use of cryptocurrencies is perceived as controversial. Any subject, e. g. person liable/natural person/state) can be affected by illegal activities related to the use of cryptocurrencies. The use of cryptocurrencies for criminal purposes and with the harmful effects to the involved parties is becoming more problematic even in the light of new emerging information from the real-life situations. As the new threats and risks are currently present in the area of cryptocurrency use, the authors of the present study decided to present available information from practice and analyze it in order to not only expand the reader's knowledge but also suggest particular recommendations in regard to police theory and practice.

## Risks of using virtual currencies

The European Banking Authority (hereinafter referred to as 'EBA') identifies a number of risks that occur individually for different market participants in virtual currency systems and areas related to it, the following are some of the examples:

- risks related to users of virtual currency (buyer, seller);
- risks associated with other participants in the virtual currency market (exchange platforms);
- risks related to crime (money laundering and terrorist financing, financial and other crimes);
- risks associated with existing payment systems;
- risks related to the regulation and supervision of the virtual currency market.<sup>1</sup>

The users or actors involved in buying, holding, or trading virtual currencies are exposed to several risks, such as:

- **credit risks:** in all circumstances, those who lend in exchange for a virtual currency may run into problems, as it is uncertain whether the cryptocurrency issuer will be able to meet its outstanding obligations to the creditor. An obvious example is the bankruptcy of a currency exchange platform;

- **liquidity risks:** the virtual currency has extremely low liquidity and its value is based on supply and demand, which means high volatility of value (volatility);

- **operational risks:** it is usually associated with the stable and secure operations of the virtual currency issuer and is related to the operation of the scheme itself. Although many cryptocurrency systems, including transactions, exchanges, and darknet traders, are anonymous and well-protected, it is also likely that any skilled and sophisticated IT professional can find a loophole in the system and then break into the exchange platform;

- **legal risks:** in general, there is legal uncertainty in the functioning of the cryptocurrency platform mechanism.<sup>2</sup>

---

<sup>1</sup> Alternativne bankové platformy, 2015, p. 39.

<sup>2</sup> Alternativne bankové platformy, 2015, p. 40 and following.

## Virtual currencies versus crime

Experts often predict problems of existential, financial, but also legislative nature for virtual currencies. In this context, it is appropriate to answer some questions, such as who issues the virtual currency, what is a price of cryptocurrency based on, who recognized it at all and how it is handled, how it should be used, but also how it is abused, whether the crime may be related to it.

The existence of Bitcoin, for example, gave rise to a new type of malware. Malicious programs may not only be affected by data theft but also those that "*steal the computing power*" of an infected computer by exploiting cryptocurrencies. Not least, the untraceable bitcoins facilitate the commission of so-called "*classical*" crime, such as extortion or kidnapping.

The more sophisticated ways are used in the commission of criminal offenses, including the transfer of financial resources through alternative banking platforms which may be understood as virtual bank accounts that operate outside the regulated global financial sector. Just alternative banking platforms may become the intermediary in monetary transfers - small or even large amounts of money may help to legalize financial resources consequently used for the criminal activities or the purchase of software, false documents, credit cards, etc. The most frequently funded criminal activities are economic and financial frauds or organized terrorist activities. Today, the use of the financial resources obtained in such a manner is common in perpetrators.

Although virtual currencies appear to be a future trend in payment systems, the risk associated with their use and legalization in the business world is worth monitoring. Today, cryptocurrencies provide a new, powerful tool - even for criminals - to transfer and store money from crime. In addition, they represent important means of financing terrorism outside the reach of law enforcement authorities and other bodies regulating financial markets and banking systems.

Unlike "*real money*" – so-called "*fiat money*", virtual currencies can be used to quickly invest, buy, and sell with just a single click. Although virtual currencies are attractive means of payment for any investment, cryptocurrency-based payment products and services open the door to unlimited opportunities to launder the proceeds of crime and terrorist financing.

However, virtual currency is not the only means used in committing the crime. Perpetrators have a number of different applications and tools at their disposal, through which they can, for example, conceal their identities, transactions, and communication channels, data stored on hard disks, as well as the payments.

The indicated, relatively new, phenomenon of crime requires the law enforcement authorities and related financial or banking institutions and regulators to take a step forward or at least keep pace with the most recent developments in illegal practices.<sup>1</sup>

Virtual currency is not money or currency from a legal perspective. It is not officially recognized as having domestic legal tender status, which means that it is not issued or guaranteed by any jurisdiction. The legalization of currency status is subject to agreement in the community of virtual currency users.

---

<sup>1</sup> Alternativne bankové platformy, 2015, p. 7 and following.

In the case of convertible virtual currencies, convertibility makes them an uncovered (*fiat*) goal or means through which illegal activities such as money laundering or illegal financial transactions may be executed.

To better understand the perpetrators' actions, it is appropriate to become familiar with the mechanisms that bring them greater opportunities, i.e. whether virtual currencies are managed by a centralized system or not.

In risk assessments and investigations, the law enforcement authorities mostly focus on decentralized virtual currencies known as cryptocurrencies, because they are open-source virtual currencies that are based on the principle of a decentralized electronic payment system.<sup>1</sup>

In order to increase the success of clarifying illegal activities related to cryptocurrencies, it is appropriate for law enforcement authorities to know the key actors that are participating in the process. The "ecosystem" of virtual currency schemes consists mainly of specific, new categories of actors that were not present in the payments environment before. Among the most relevant ones are "an issuer", "a user" and "a wallet provider". The European Central bank issued in 2015 detailed description of the key actors. The descriptions are part of the material *Virtual Currency Schemes – a further Analysis* (February, 2015). The descriptions of the relevant key actors are as follows:

**Issuers** are able to generate units of the virtual currency. Depending on the design of the VCS, the total issuance volume is predetermined or depends on demand. In centralized VCS, the issuer is often also the administrator of the VCS which establishes the rules for its usage and has the authority to withdraw units from circulation. Once units have been issued, they are normally delivered to users, either by selling them or by distributing them free of charge.<sup>3</sup> In decentralized VCS, new units can be created automatically as the result of the activities performed by "miners", who receive these units as a reward.<sup>2</sup>

**Users** choose to obtain virtual currency for purchasing virtual or real goods and services from specific merchants, for making person-to-person payments (e.g. cross-border) or sending remittances, or for investment purposes, including speculation. There are five ways to obtain units: 1) purchase; 2) engage in activities that are rewarded with units of virtual currency (e.g. filling out a survey, participating in the promotional activity); 3) self-generate units of the currency by acting as a miner ("mining"); 4) receive units as a payment; or 5) receive units as a donation/gift.<sup>3</sup>

**Wallet providers** offer a digital wallet to users for storing their virtual currency cryptographic keys and transaction authentication codes, initiating transactions, and providing an overview of their transaction history. There are basically two types of wallets, which differ as regards their immediate usability versus their safety from cybercrime: online wallets (hot storage) and offline wallets (cold storage). From a functional perspective, these services are offered for desktop PCs, mobile devices,

---

<sup>1</sup> Alternativne bankové platformy, 2015, p. 8 and following.

<sup>2</sup> Virtual currency schemes – a further analysis. Available online at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> [cit. 2020-07-03].

<sup>3</sup> Virtual currency schemes – a further analysis. Available online at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> [cit. 2020-07-03].

and as cloud-based applications. Nevertheless, users can also set up and maintain a wallet themselves without making use of a wallet provider.<sup>1</sup>

The anonymity of payments is a tempting advantage that provides a space for transfers of financial resources generated from criminal and illegal activities (money laundering, terrorist activities, tax evasion, etc.). Although the same possibilities are currently provided by cash payments, cryptocurrency transmissions bring additional advantage in the form of a public database of all payment transactions. There are certain persons – so-called miners who voluntarily make computer processing available in order to validate a set of transactions (called a “block”) made with a decentralized VCS and add this to the payment ledger (called a “blockchain”); without miners, the decentralized VCS would not run smoothly, since double-spent or false units could easily be introduced. As a reward for their work, miners normally receive a specific number of units.<sup>2</sup> Thus, even the persons registered in this database remain unknown there is still a possibility to track down their identity by analytical processing of data.<sup>3</sup>

At a practical level, it is important to be aware of the fact (also confirmed by the Slovak experts) that the detection of crimes in which virtual currencies are misused to commit the crime (e.g. terrorist financing) or are misused to cover up the origin/proceeds of crime (i.e. legalization of proceeds from crime) takes place on the basis of how the law enforcement authorities find out about the criminal activity (illegal activity). There is a number of ways in which the law enforcement authorities may detect cryptocurrency abuse, e.g. the police's own 'operational search activities'; notification of a suspicious financial transaction by a particular financial institution; examining the information pointed out by investigative journalists in the media; filing a criminal complaint that a criminal offense has been committed by a specific person; exchange of information from international partners or investigation of predictive crimes.<sup>4</sup>

## **Virtual currencies and "darknet"**

Darknet has undergone great development. A few years ago, stolen credit cards were mainly sold in hidden markets, and transactions took place in person. Today, darknet works as a convenient secret shopping portal where one can trade weapons, drugs, or fake documents. The sale of stolen personal data or counterfeit banknotes (which are sold with advice on how to put them into circulation) may also be a widespread darknet business. In principle, you can simply empty the shopping cart by payment in Bitcoin. This relatively unpretentious model results in a gradual increase in the number of stores offering 'illegal gifts' on the darknet. The prices of goods are stated in bitcoins, but also in US dollars - for better customer orientation.<sup>5</sup>

---

<sup>1</sup> Virtual currency schemes – a further analysis. Available online at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> [cit. 2020-07-03].

<sup>2</sup> Virtual currency schemes – a further analysis. Available online at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> [cit. 2020-07-03].

<sup>3</sup> Alternatívne bankové platformy, 2015, p. 14 and following.

<sup>4</sup> The relevant information was provided by the experts and the best practice.

<sup>5</sup> Alternatívne bankové platformy, 2015, p. 21 and following.

## Theoretical Preliminaries

### Legislation, Formal Scope and Selected Activities of Competent Authorities in Slovakia within the European Framework

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 purpose of money laundering or terrorist financing does not omit the issue of virtual currencies.

Pursuant to Art. 4 of the above-mentioned Directive, the prevention of money laundering and terrorist financing can only be effective in an environment that does not assist perpetrators seeking shelter for their finances through non-transparent structures. The aim of Directive 2015/849 is not only to detect and investigate money laundering but also to prevent its occurrence. Increasing transparency could be a strong deterrent.<sup>1</sup>

According to Stieranka et al., in general, money laundering is defined as the process of converting the proceeds of crime into legal assets through the use of a legal financial system. The legislative interpretation of the issue forms an integral part of both international and the Slovak national legislation.<sup>2</sup> As a document of particular relevance, Act no. 297/2008 Coll. on protection against money laundering and protection against terrorist financing and on amendments to certain laws pursuant to Criminal law is frequently cited and implemented in the Slovak Republic, where money laundering is defined in Section 233 of Act no. 300/2005 Coll. Criminal law.

A number of central banks, supervisory authorities, and other government agencies around the world have communicated publicly on VCS. There are a general tendency and many efforts to have the authority to regulate VCS (the most frequently Bitcoin) in any way. Germany can serve as an example of such an effort as bitcoins are not recognized as a currency. In Germany, bitcoins are labeled only as '*privates Geld*' and the preconditions for their further regulation were set. The main motivation behind those steps was the aim to prevent tax evasion, as the bitcoin trade in the country is growing significantly, and due to the significant appreciation of its exchange rate (at the time of this publication the exchange rate of Bitcoin was USD 11 315,35) against the dollar (see Table 1),<sup>3</sup> it was possible to generate a relatively large income by selling it, while the sale was not taxed.<sup>4</sup>











---

<sup>1</sup> 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.

<sup>2</sup> STIERANKA, J. et al., 2018. *Legalizácia príjmov z trestnej činnosti a financovanie terorizmu*, p. 14 and following.

<sup>3</sup> See <https://coinmarketcap.com/> [cit. 2020-08-23].

<sup>4</sup> See NBS.sk. Available online in SK at [https://www.nbs.sk/\\_img/Documents/\\_PUBLIK\\_NBS\\_FSR/Biatec/Rok2013/08-2013/06\\_biatec13-8\\_nadasky.pdf](https://www.nbs.sk/_img/Documents/_PUBLIK_NBS_FSR/Biatec/Rok2013/08-2013/06_biatec13-8_nadasky.pdf) [cit. 2020-07-03].

Rank	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$209 003 212 915	\$11 315,35	\$25 629 318 258	18 470 775 BTC	-3,66%	
2	 Ethereum	\$42 545 043 454	\$378,75	\$12 359 713 191	112 330 255 ETH	-6,02%	
3	 XRP	\$12 372 525 308	\$0,275296	\$1 376 815 456	44 942 589 751 XRP *	-4,36%	
4	 Tether	\$10 043 584 506	\$1,00	\$41 387 336 781	9 998 221 723 USDT *	0,35%	
5	 Bitcoin Cash	\$5 076 210 256	\$274,40	\$1 436 379 882	18 499 613 BCH	-5,33%	

**Table 1** Exchange rates of the top 5 Cryptocurrencies by Market Capitalization.

In order to address threats (for example in relation to the free movement of criminals, terrorists, proceeds of crime and financial resources for terrorism) at the European level, the Financial Intelligence Units of France, Italy, Luxembourg, and the United Kingdom joined in 2002 the vision of the Dutch Financial Intelligence Units to create an information network of Financial Intelligence Units (hereinafter referred to as 'FIU'). Creating greater synergies between financial and criminal intelligence (FIU.net) ultimately increases efforts to combat the most serious crime.

The Financial Action Task Force (hereinafter referred to as 'FATF') also has an irreplaceable role in coordinating measures to combat money laundering and financing of terrorist activities. FATF was established to set standards and support the effective implementation of regulatory and legal measures aimed at combating money laundering and terrorist financing and other threats to the integrity of the international financial system.

The Egmont Group, Interpol and Europol initiated meetings of the Cryptocurrency Working Group, where the representatives of competent FIUs, the law enforcement authorities and the private sector exchange technical skills and experience in connection with cryptocurrency. Joint proposals are drafted with the aim to regulate digital exchange offices and digital wallet providers, definitions of the cryptocurrency concepts, cryptocurrency exchanges, etc. are tackled in order to form an integral part of the European legislation.

The attention to cryptocurrency is paid also in the territory of the United States of America where the Financial Crimes Enforcement Network (FinCEN, in particular, the Department of Treasury) is responsible for the investigation of the cryptocurrency crimes committed in the territory of the USA.<sup>1</sup>

In order to fight crime successfully and effectively, it is necessary to create a comprehensive, compact system of institutions at different vertical levels that will be able to use different tools, means, and procedures to eliminate money laundering, terrorist financing, and other criminal activities. The corresponding levels should

<sup>1</sup> UJVÁRY, K. et J. KUČTOVÁ, 2019. *Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom*, p. 186 and following.



include: **person liable** (first vertical level), **FIUs** (second vertical level), **the law enforcement authorities** (third vertical level).<sup>1</sup>

### **Application Practice in the Slovak Republic and the Interview Process**

In the context of the Slovak Republic, with regard to the subject matter in the system of institutions, the FIU plays an important role. The most important part of the FIU's activities is focused on receiving, analyzing, evaluating and processing reports on unusual business operations (hereinafter referred to as 'UBO') - based on the statutory reporting obligation arising from the Anti-Money Laundering Act (hereinafter referred to as 'AML Act'), from persons liable defined in this Act (especially banks, other financial institutions or non-financial institutions).

FIU of the National Criminal Agency of the Presidium of the Police Force in its annual report provides a comprehensive view of the present developments in the fight against the legalization of proceeds from criminal activities and terrorist financing in the Slovak Republic including defining of forecasts of their further development and direction. Based on the analysis of the obtained information and current situation in the Slovak Republic, the following activities and development of trends in money-laundering and countering the financing of terrorism (hereinafter referred to as 'ML/CFT') may be predicted, in particular, with the focus on activities generating income (among others) from the abuse of cryptocurrency, electronic wallets, and electronic payment gateways.

In 2019, FIU drafted an amendment to the AML Act, while the main objective was the transposition of Directive 2018/843 of the European Parliament and of the Council and the acceptance of Moneyval and FATF recommendations, in an effort to respond effectively to ongoing developments in the fight against ML/CFT. The draft was aimed to improve access to beneficial ownership registers in general, but also to strengthen and harmonize rules for customer due diligence, to take stricter measures to reduce the ML/CFT risks associated with unknown prepaid instruments, and to monitor UBOs through virtual cryptocurrencies, politically exposed persons and to elaborate in detail the FIU's procedure for exchanging information with the competent authorities of the Member States of the European Union that are needed to prevent and detect ML/CFT.<sup>2</sup>

The Cyber Crime Department from the Office of Criminal Police of the Police Force Presidium is an equally important institution in the Slovak Republic. Regardless of the development of the situation related to the legal status and nature of cryptocurrencies or the protection of the cryptocurrency ownership, it is already necessary for the law enforcement authorities to be able to respond to the challenges related to cryptocurrency in the context of the national criminal proceedings (in which it is necessary to ensure appropriate response and, if necessary, to secure cryptocurrencies, i.e. to remove the owner's disposition options), and in the context of international judicial cooperation.

---

<sup>1</sup> STIERANKA, J. et al., 2018. *Legalizácia príjmov z trestnej činnosti a financovanie terorizmu*, p. 118 and following.

<sup>2</sup> Annual Report, 2019, Financial Intelligence Unit, p. 22.

Bitcoin still appears to be the most prominent of these VCS, as it accounts for more than 80% of the market capitalization of around 500 known decentralized VCS.<sup>1</sup> Bitcoin must be perceived as computer data and the bearer of property value, always in quantitative terms, in real-time. The assessment of Bitcoin/cryptocurrency as a real-time computer asset is necessary to ensure the protection of the rights and interests of individuals, legal persons and the state by legal means, and also for effective international criminal cooperation and the fulfillment of the international commitments concerning the Slovak Republic.

Pursuant to the Slovak legislative acts (from 2019) the Cyber Crime Department from the Office of Criminal Police of the Police Force Presidium is responsible for detection and documentation of the cybercrime cases with regard to the nature of the case, the way crime is committed, the affected parties or other overriding interests, and is also responsible for the operation and maintenance of the electronic wallets for the purposes of securing cryptocurrencies. The Cyber Crime Department from the Office of Criminal Police of the Police Force Presidium also manages the activities related to securing of cryptocurrencies and organizes specialized education in this area.

The analysis and understanding of the rules of operation of digital markets, and especially virtual currencies, is essential for the effective implementation of crime control in the form of both, prevention and repression.

### **Examples of the best practice from the Slovak Republic**

*'Fraudulent site abuses Aktuality.sk, Slovenská sporiteľňa and the name of a well-known entrepreneur' (February 2020, SK)*

The fraudulent site pretended to be the news portal Aktuality.sk, mentioned Slovenská sporiteľňa and highlighted the logos of other well-known Slovak media at the forefront, only to draw visitor's attention to the fraudulent business. The scam site attracted potential victims through sponsored links on Facebook. If the visitor clicked on the link, one was redirected to a fake page that was reminiscent of the Aktuality.sk website. Clicks from the site then led to the Bitcoin Era project, where a visitor was encouraged to open an account. The website was available in Slovak and English. The Bitcoin Era platform falsely informed about cooperation with Slovenská sporiteľňa. Slovenská sporiteľňa distanced itself from the above-mentioned activities and warned clients not to get deceived.<sup>2</sup>

*'Cryptocurrency mining' (August 2018, SK - Humenné District Department)*

In August 2018, an unknown perpetrator lured € 2,300 on a social network from 34-year-old Ján. By mutual agreement, Ján paid the amount via Internet banking from his bank account to the account of 'the seller'. According to the agreement, the seller

---

<sup>1</sup> Virtual currency schemes – a further analysis. Available online at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> [cit. 2020-07-03].

<sup>2</sup> O mediach.com. Available online in SK at <https://www.omeiach.com/hoaxy/17210-podvodna-stranka-zneuziva-aktuality-sk-slovensku-sporitelnu-a-meno-znameho-podnikatela> [cit. 2020-07-02].

was supposed to send the hardware in question after receiving the financial resources. The agreement has not been respected.<sup>1</sup>

*'The Slovak citizen blackmailed Dutch company' (February 2018, SK - Dolný Kubín district/the Netherlands)*

The Slovak police joined the Dutch police in search of a Slovak national who allegedly blackmailed a foreign company. The Slovak national asked the Dutch company for bitcoins in return for not being blackmailed. Police officers from Žilina were able to locate and apprehend the Slovak national in the district of Dolný Kubín.

He won't have that opportunity so soon. The 32-year-old man ended up in the hands of the law. An investigation of blackmailing is ongoing in the Netherlands. The strategy of the Slovak perpetrator was to blackmail the Dutch company in question until bitcoins are provided into his bank account. When the Dutch company refused to pay the required amount of bitcoins, the perpetrator threatened to publish the sensitive data that he had claimed he had at his disposal.<sup>2</sup>

## Interview outcomes and discussion

Members of the Cyber Crime Department from the Office of Criminal Police of the Police Force Presidium have so far only encountered such criminal activities in which the cryptocurrencies bitcoin (BTC) and ripple (XRP) have been misused or stolen.

In general, (without pointing to a specific case), the following are the examples of *modus operandi*:

- **blackmail** (the perpetrator contacts the selected victim via a social network, forms a love affair with the victim and later asks the victim for financial resources in the cryptocurrency bitcoin on the basis of various emotional stories - the so-called 'romance scam');
- **fraud** - purchase of goods for the cryptocurrency – usually bitcoin (a mobile phone purchased through an Internet advertising portal/e-shop - fraud - goods not delivered);
- **ransomware** (the perpetrator infects the victim's computer with malicious software and encrypts the data files located on the storage device, then requests a ransom in the form of cryptocurrency bitcoin for decrypting the files);
- **payments for counterfeit loans** (payment of a fee for the provision of a loan in the form of a regular cash deposit to the account of a *straw man*, subsequently the account holder (straw man) withdraws the money and deposits the money at the bitcoin address via a bitcoin machine);
- **purchase and sale of illegal goods through darknet markets** (weapons, drugs, child pornography, counterfeit documents, counterfeit notes, etc.).<sup>3</sup>

---

<sup>1</sup> Minv.sk. Available online in SK at <http://www.minv.sk/?aktuality-presov&sprava=tazba-kryptomeny> [cit. 2020-07-02].

<sup>2</sup> Techbyte.sk. Available online in SK at <https://www.techbyte.sk/2018/02/slovak-kryptomeny-kryptomena-bitcoin-vydieranie-holandsko/> [cit. 2020-07-02].

<sup>3</sup> The relevant information was provided by the experts and the best practice.

Due to the specificity of the issue, police knowledge about the issue is modest - both qualitatively and quantitatively. The Slovak police do not record the number of illegal acts associated with cryptocurrencies. Even the cryptocurrency crimes would be registered and listed, they would be subject of confidentiality. From a qualitative point of view, the Slovak police also did not deal with particularly serious and large cases related to cryptocurrencies and cybercrime. There are several reasons. Probably the most significant is the fact that people are not wealthy enough to own cryptocurrencies. The Slovak police has not been dealing with crimes related to cryptocurrency on daily basis, thus in such cases solutions need to be consult in advance with the competent authorities and foreign partners at least at the European or international level as the Slovak Police Force has limited resources in personnel, knowledge base, financial and others. However, distribution of the knowledge and experience gained so far within the territory of the Slovak Republic might contribute to the best practice sharing with other countries. The given information might help to create a new, added and slightly improved picture about the state of art in the field of crime related specifically to cryptocurrency.

The interview process facilitated the basic information sharing and contributed to the spreading of already existing data. The data being made publicly available to the larger audience can help to improve not only the current knowledge base but also can contribute to the measures development that would consequently assist in decreasing the level of criminal activities. Knowledge-based and well-oriented units of the Police Force might be helpful also in the field of prevention. So far, the information and knowledge from abroad was passed to the Slovak Police Force. However, due to different conditions and legal measures the implementation of the theoretical knowledge and practical information from foreign countries was not possible in the conditions of the Slovak Republic.

The current knowledge presented in the framework of this study might find its audience very quickly as the relevant data might be used to set the minimum standards in the field of cybercrime combat with cryptocurrency crimes being also taken into account.

The main aim of the presented contribution was to facilitate and mediate the relevant data to all competent individuals and organization/institutions that can process the gained data for the purposes of fight against the crime and at the same time assisting in developing and improvement of preventive but also restrictive measures that might be applicable in the nearby future in the territory of the Slovak Republic in the area of cryptocurrency related crimes.

By presenting the respective outcomes of the interview, the authors fulfilled the initial objective to provide the relevant data and facilitate further measure development and prevention setting in the above-mentioned field.

## **Conclusion**

Changes in the practices and methods of committing profit-driven crimes happen quicker than ever and perpetrators are drawn from a wider spectrum of society. Thus, changes in techniques of prevention, detection, and investigation are required from the law enforcement authorities in order to reflect the current status quo of crime and to keep up with the recent developments in the crime area.

There are several factors present that led to the emergence of a new cross-border nature of the digital crime. To the large extent, the globalization and the use of Internet gave rise to different types of crime such as e-commerce fraud (online operations or payments), virtual currencies used as a financial settlement in criminal activities (illicit trafficking of drugs, arms, stolen goods, people, stolen and counterfeit documents, child pornography) and money laundering.

The criminal activities related to virtual currencies are also one of the most recent trends as the anonymity of the payee, the lack of transparency, clarity and continuity, the high volatility of the exchange rate, high dependency on the IT and on networks and above all the absence of the supervisory authority in this field present a tempting environment for criminals.

The general advantages of virtual currencies as they are perceived by users are costs, global reach, the anonymity of the payer, and speed of settlement. The drawbacks and disadvantages of virtual currencies are discussed less frequently, but there are certain risks associated with certain intrinsic characteristics of virtual currencies and there are currently no safeguards to protect users against these risks.

The rapid and unobservable transfer of financial resources anywhere in the world and the overall anonymity of the cryptocurrency system have become a breeding ground for virtual currencies to become the only real currency in the electronic black market.

Just as technology facilitates crime, on the one hand, it also helps to detect it on the other. Advances in data analysis suggest that technological solutions play a crucial role in the fight against this type of crime. Technologies allow the law enforcement authorities, for example, to set alerts, monitor suspicious transactions, and initiate deeper investigations.

The growing use of new technologies in crime-related activities poses a greater challenge for the law enforcement authorities in the Member States of the European Union. Financial crimes are transnational and complex and are increasingly being committed by using virtual cryptocurrencies as trading tools on the stock exchange.

In order to combat serious and organized crime effectively, it is necessary to constantly expand the knowledge, information, and competence of the law enforcement authorities for the purposes of detecting various financial crimes and the interconnections within the globalized financial environment.

Organized perpetrators of cybercrime will continue to develop their capabilities, including the acquisition of innovative forms of information and communication technologies to support financial crime. But thanks to advanced forms of investigative analysis, law enforcement authorities can increase the ability to identify individuals and organizations, and therefore strengthen the effective and successful fight against these types of crimes.

Based on the analysis and study of the available literature, it is obvious that each state so far approaches the issue of cryptocurrency differently. Differences in national

prohibitions, regulations, and tax structures open opportunities for transnational crime.<sup>1</sup>

The experts from the Cyber Crime Department from the Office of Criminal Police of the Police Force Presidium look at the issue of virtual currencies as follows:

*'It is undoubtedly extremely necessary to deal with the topic of cryptocurrencies and the investigation of cryptocurrency-related crime, as they are increasingly being misused in various types of crime (ransomware, terrorist financing, money laundering, fraud, etc.). This is due to the fact that perpetrators have many times a higher sense of anonymity, as they believe it is extremely difficult for the police to track the flow of transactions (for example when bitcoin is used to commit the crime) due to the complexity of transactions in a blockchain database - without specific software developed for tracing. bitcoin transactions, or due to the use of services such as the so-called "mixer", or the transformation of cryptocurrencies on online exchange markets (sale of one cryptocurrency and purchase of another cryptocurrency). In addition, perpetrators benefit increasingly from the use of anonymization networks, anonymization VPN services, anonymous remailer servers, cryptocurrencies, which makes it significantly more difficult to investigate this crime.*

*In addition, the current practice shows that the perpetrators of this crime are rapidly adapting to the use of completely anonymous cryptocurrencies, such as the cryptocurrency Monero. An example is the payment for ordered goods with the cryptocurrency Monero in the darknet markets Empire, Berlusconi, Cryptonia. We also see a large increase in fraudulent websites that promise to get rich by trading in cryptocurrencies such as Bitcoin Revolution, Bitcoin Era, Bitcoin Billionaire, and s on.'*

Experts from many countries list the challenges of financial investigations involving cryptocurrencies. In the Slovak Republic, experts from practice emphasize, in particular, the following challenges:

- problems associated with proving that cryptocurrencies are the proceeds of crime;
- analysis of cryptocurrency transactions is challenging must be justified, explained and recognized before the court;
- issues related to the use of completely anonymous cryptocurrencies, such as the cryptocurrency Monero;
- problem with foreign cryptocurrency stock-exchange – information requests, orders to issue and store computer data requires international legal assistance;
- facts related to anonymity within the Internet and the world of cryptocurrencies - anonymous registration on cryptocurrency stock-exchange (e.g. VPN/TOR/false documents), use of bitcoin ATMs, which are relatively anonymous, insufficient implementation of the "Know Your Customer" ('KYC') security policy) on online cryptocurrency exchanges and the overall lack of cryptocurrency legislation in some countries (regulation of the conditions for companies offering such services);

---

<sup>1</sup> See [https://www.justice.gc.ca/eng/rp-pr/csj-sjc/crime/rr03\\_20/p1.html](https://www.justice.gc.ca/eng/rp-pr/csj-sjc/crime/rr03_20/p1.html) [cit. 2020-08-23].

- the challenge for the future – to increase the level of education for the members of the Police Force, prosecutors, and judges in the subject matter.<sup>1</sup>

The international nature of cybercrime requires enhancing the cooperation with the partner FIUs, in particular, in the neighboring countries, and to improve own knowledge in the fight against the legalization of proceeds from criminal activities and terrorist financing by making use of information and experience shared by the partners. To combat the cybercrime successfully and efficiently the law enforcement authorities are required to operate promptly and effectively. Thus, the results of the law enforcement activities depend on the quality of coordination of activities of all partners involved in the fight against the legalization of proceeds from criminal activities and terrorist financing.

## Literature

Annual report, 2019, Financial Intelligence Unit.

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.

Ecb.europa.eu. Available online at

<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> [cit. 2020-07-14].

Eds. 2015. *Alternatívne bankové platformy*. Brožúra. Vydané ako súčasť projektu KNOWLEDGE ENHANCEMENT AND OPERATIONAL CAPACITY PEINFORCEMENT ON MTIC FRAUDS.

Interviews conducted with the Cyber Crime Department Experts from the Office of Criminal Police of the Police Force Presidium.

Minv.sk. Available online at <http://www.minv.sk/?aktuality-presov&sprava=tazba-kryptomeny> [cit. 2020-07-02].

Minv.sk. Available online in SK at [https://www.minv.sk/?Egmont\\_Group-1](https://www.minv.sk/?Egmont_Group-1) [cit. 2020-06-30].

NBS.sk. Available online in SK at

[https://www.nbs.sk/img/Documents/PUBLIK\\_NBS\\_FSR/Biatec/Rok2013/08-2013/06\\_biatec13-8\\_nadasky.pdf](https://www.nbs.sk/img/Documents/PUBLIK_NBS_FSR/Biatec/Rok2013/08-2013/06_biatec13-8_nadasky.pdf) [cit. 2020-07-03].

O mediach.com. Available in SK online at <https://www.omeiach.com/hoaxy/17210-podvodna-stranka-zneuziva-aktuality-sk-slovensku-sporitelnu-a-meno-znameho-podnikatela> [cit. 2020-07-02].

SABAYOVÁ, M. et M. PRESPERÍNOVÁ, 2018. Vybrané riziká prania špinavých peňazí a financovania terorizmu. *Policajná teória a prax*. Edition XXVI, Vol. 1. Bratislava: Academy of the Police Force in Bratislava, p. 124-132. ISSN 1335-1370.

SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, Ltd. 2015. 636 p. ISBN 978-80-7380-501-2.

---

<sup>1</sup> The relevant information was provided by the experts and the best practice.

- STIERANKA, J. et al. *Legalizácia príjmov z trestnej činnosti a financovanie terorizmu, právna a inštitucionálna ochrana v Slovenskej republike*. Bratislava: Wolters Kluwer SR, s. r. o. 2018. 193 p. ISBN 978-80-8168-912-3.
- ŠIŠULÁK, S. et L. JAKUBÍK, 2016. *Virtuálne meny v procese legalizácie príjmov z trestnej činnosti*, In Aktuálne otázky trestného práva v teórii a praxi, 4<sup>th</sup> edition of the Interdisciplinary national scientific conference with international participation (Collection of papers). Bratislava: Academy of the Police Force in Bratislava, p. 267-279, ISBN 978-80-8054-682-3.
- Techbyte.sk. Available online in SK at <https://www.techbyte.sk/2018/02/slovak-kryptomeny-kryptomena-bitcoin-vydieranie-holandsko/> [cit. 2020-07-02].
- UJVÁRY, K. et J. KUČTOVÁ, 2019. *Špecifická objasňovania finančných transakcií v súvislosti s bitcoinom*, In Collection of papers from the Scientific conference with the international participation held in Bratislava, 4 June 2019, Bratislava: Academy of the Police Force in Bratislava, p. 185 – 195. ISBN 978-80-8054-820-9.
- Virtual currency schemes – a further analysis. Available online at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>.
- Zakony pre ludi.sk. Available online in SK at <https://www.zakonypreludi.sk/zz/2008-297> [cit. 2020-06-28].

## RESUMÉ

*JURISOVÁ, Michaela; NIKOLAJOVÁ KUPFERSCHMIDTOVÁ, Elena: VIRTUÁLNE MENY VERZUS ZLOČIN V KONTEXTE SLOVENSKEJ REPUBLIKY*

Predkladaná štúdia sa venuje problematike kryptomien, pričom pozornosť je sústredená predovšetkým na predstavenie pozitívnych stránok, ale aj negatívnych dopadov využívania kryptomien vo vzťahu k trestnej činnosti páchanej v tejto oblasti na území Slovenskej republiky a možnostiam a spôsobom vyšetrovania súvisiacich trestných činov zo strany polície. S cieľom priblížiť problematiku kryptomien a počítačovej kriminality, autorky čerpali nielen z aktuálnej odbornej vedeckej literatúry a právnych predpisov, ale taktiež realizovali početné rozhovory s odborníkmi z aplikačnej praxe, a to predovšetkým s expertmi z odboru počítačovej kriminality Úradu kriminálnej polície Prezídia Policajného zboru. Prezentáciou získaných údajov a konkrétnych trestných činov, s ktorými sa policajné zložky na území Slovenska musia v oblasti počítačovej kriminality vysporiadať tvoria podstatnú časť predkladanej štúdie. S ohľadom na výstupy z realizovaných rozhovorov autorky upozorňujú na nevyhnutnosť posilnenia medzinárodnej spolupráce medzi príslušnými orgánmi a potrebu zvýšenia povedomia o počítačovej kriminalite nielen medzi členmi Policajného zboru, ale aj medzi prokurátormi, sudcami a širokou verejnosťou.

**Kľúčové slová:** virtuálna mena, kryptomena, bitcoin, kriminalita, legislatívny rámec, príslušné orgány, Slovenská republika.



## **S U M M A R Y**

The present paper is dedicated to cryptocurrencies while their advantages and disadvantages are presented in relation to police work and the ways a cybercrime is tackled in the territory of the Slovak Republic. In order to get as detailed information as possible, not only the scientific and legal literature was analysed but also the interviews with the members of the Cyber Crime Department of the Police Force Presidium were conducted. Thus, the authors were able to present the ways crimes related to virtual currency, e.g. money laundering, terrorist financing, human trafficking or tax evasion, are tackled by the Police Force in Slovakia. However, as a result from the gained data, the need for further analysis and research in the area of cybercrime is presented as of crucial importance along with the need to enhance the international cooperation between relevant authorities and to increase the level of education for the members of the Police Force, prosecutors, and judges in the subject matter

**Key words:** virtual currency, cryptocurrency, Bitcoin, crime, legislative framework, competent authorities, the Slovak Republic.

