HANDBOOK FOR DEALING WITH
VIRTUAL CURRENCIES IN CRIMINAL PROCEEDINGS

OSCE Organization for Security and Co-operation in Europe
Mission to Skopje

AJPP
Academy for Judges and Public Prosecutors

Handbook for dealing with virtual currencies in criminal proceedings

Publisher: OSCE Mission to Skopje

Authors: Lenche Ristoska, Anita Veternik

Editors: Artan Murati, Gjorgji Koneski

Translation and proofreading: "Bestel"- Skopje

Graphic design: "Polyesterday", Skopje

ISBN: 978-92-9271-026-2

OSCE Organization for Security and Co-operation in Europe
Mission to Skopje

Handbook for dealing with virtual currencies in criminal proceedings

Table of content

Acronyms and abbreviations 6

I. Introduction 8

II. Concepts and definitions 10

1. Virtual currencies 10
   1.1. Convertible and non-convertible virtual currency 12
   1.2. Centralized and decentralized virtual currency 13
2. Virtual currency system participants 14
   2.1. Coin inventors and administrators/issuers 14
   2.2. Mining and miners 15
   2.3. User 17
   2.4. Exchanger 17
   2.5. Trading platforms 19
   2.6. Virtual currency wallet 19
   2.7. Wallet provider 22
   2.8. Seed 23
   2.9. Payment providers 23
   2.10. Anonymizer (anonymizing tool) 23
   2.11. Mixers and tumblers 23
   2.12. Tor 25
   2.13. VPN 25
   2.14. Bitcoin 25
   2.15. Altcoin 26
      2.15.1. Mining-Based cryptocurrencies 26
      2.15.2. Stablecoins 26
      2.15.3. Security tokens 27
      2.15.4. Utility tokens 27
3. How the concept of virtual currencies is put in practice 27

III. Importance of virtual currencies in criminal proceedings 28

1. Detecting virtual currencies in criminal proceedings and obtaining relevant information and evidence 28
2. Obtaining control over virtual currencies 31

IV. North Macedonia legislation regarding virtual currencies 34

1. National legal grounds for dealing with virtual currencies in criminal proceedings 35

1.1. Seizure and confiscation of virtual currencies as instrumentalities of crime 36

1.1.1. Seizure of virtual currencies as instrumentalities of crime 37

1.1.2. Confiscation of virtual currencies as instrumentalities of crime 40

1.2. Seizure and confiscation of virtual currencies as proceeds of crime 42

1.2.1. Seizure of virtual currencies as a proceeds of crime 42

1.2.2. Confiscation of virtual currencies as proceeds of crime 44

1.3. Virtual currencies as evidence in criminal proceedings 45

2. International legal grounds for seizure and confiscation of virtual currencies obliging North Macedonia 48

3. Practical challenges for seizure and confiscation of virtual currencies in criminal proceedings and open questions 50

V. Republic of Slovenia experience in handling virtual currencies in criminal proceedings 53

1. Legal framework 53

2. Investigation and acquisition of information 56

3. Security of claims and confiscation of assets 58

4. Substantive criminal provisions in Slovenian legal framework 61

5. Practical experience – case study 63

VI. Conclusions and recommendations 68

Bibliography 71

Annex 76

Acronyms and abbreviations

EU	European Union
ECB	European Central Bank
FATF	Financial Action Task Force
EJCN	European Judicial Cybercrime Network
ML	Money Laundering
FT	Financing of Terrorism
VC	Virtual Currency
CBDC	Central Bank Digital Currencies
VPN	Virtual Private Network
PoW	Proof-of-Work
ICOs	Initial Coin Offerings
QR code	Quick Response Code
PIN	Personal Identification Number
IP	Internet Protocol
ID	Identity Card
CCTV	Closed-Circuit Television or Video Surveillance
UTXO	Unspent Transaction Output
MLA	Mutual legal assistance
AMLD 5	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 Purpose of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/Ec and 2013/36/Eu
ZPPDFT	Prevention of Money Laundering and Terrorist Financing Act of Slovenia

ZPlaSSIED	Payment Services, Services of Issuing Electronic Money and Payment Systems Act of Slovenia
OZ	Obligations Code of Slovenia
SPZ	Law of Property Code of Slovenia
KZ	Criminal Code of Slovenia
ZKP	Criminal Procedure Code of Slovenia
CC	Criminal Code of North Macedonia
CPC	Criminal Procedure Code of North Macedonia

I. Introduction

Virtual currencies are becoming new reality not only for the financial systems, the digital world and their users, but for law enforcement agencies and judiciary, as well. Despite their genuine existence and goal, virtual currencies are often targeted by criminals as a subject of a criminal offence or as an illicit value gained by committing criminal offences, that creates the need for law enforcement agencies to develop deeper understanding on the concept of the virtual currencies, their use and, consequently, their abuse for criminal purposes.

The Handbook for dealing with virtual currencies in criminal proceedings was developed with the support of the OSCE Mission to Skopje under the framework of the project: "Strengthening the Rule of Law and Human Rights in North Macedonia" and in cooperation with the national Academy for Judges and Public Prosecutors. The purpose of the Handbook is twofold: 1) to serve as a tool for national law enforcement agencies and the Prosecutor's Office in criminal procedures involving virtual currencies and 2) to be used as a training tool for Judges and Public Prosecutors attending training at the Academy for Judges and Public Prosecutors.

The main idea for developing this kind of Handbook lies behind the current situation in North Macedonia regarding the virtual currencies, which is more than challenging. Not being able to recognize the virtual currencies as a reality, the legislation in North Macedonia, at this moment, does not deal with virtual currencies at all. However, having in mind the interest of North Macedonia for EU integration, the EU standards and the international standards and instruments that oblige North Macedonia, at the moment of publishing this Handbook, there are legislative attempts of the national authorities of North Macedonia to define and somewhat regulate the virtual currencies. In this light, this Handbook provides theoretical insight of the concept of virtual currencies, underlines the legislative position and legislative attempts of the authorities of North Macedonia and also provides practical solutions on how to deal with virtual currencies in criminal proceedings on basis of current legislation.

Moreover, the Handbook provides information about the existent EU standards in this area and best practices, taking as example the Slovenian legislation, as a legislation similar to the one of North Macedonia, but at a same time, a legislation that is in line with all European standards. Apart from being able to deepen their understanding about the existent legal developments concerning

virtual currencies in criminal proceedings, professionals are given possibilities to learn from other countries experiences and implement best practices.

In essence, the Handbook aims to improve the capacities of law enforcement representatives in North Macedonia when dealing with virtual currencies in criminal proceedings by providing practical information for investigators and prosecutors on the detection, investigation, prosecution and seizure of virtual currencies in criminal proceedings. Having in mind that the Handbook underlines the international and EU standards in the area, combined with current national efforts, it can be also seen as a guide for the authorities in North Macedonia for drafting and adopting comprehensive and harmonized legislation for the subject of virtual currencies in criminal proceedings.

The methodology used for developing this handbook is based on legal research in the area and practical insights and experiences of the experts who developed it. Also, a series of meetings and interviews with representatives from institutions of North Macedonia that have interest in the developing of a legal framework around VC, were conducted.

The Handbook is consisted of five main chapters, including the introduction as the first chapter. The second chapter focuses on concepts and definitions that practitioners should be familiar with, in order to better understand the technology and the virtual currencies. The third chapter explains the importance of VC for the criminal proceedings and provides information and practical advice on how to detect and secure VC in criminal proceedings. The fourth chapter analyzes the legislation of North Macedonia and provides guidelines for practitioners on the seizure and confiscation of VC under the current legislation. The international obligations that North Macedonia has undertaken in relation to the seizure and confiscation of VC are also elaborated. The fifth chapter includes the experience of Republic of Slovenia, as relevant EU experience in the area of seizure and confiscation of VC. The elaborated legal framework is supported with a practical example and a case study is also included. The final chapter addresses the conclusions and the recommendations, which combine the practical experiences that exist in Slovenia and the existent legal framework in North Macedonia.

II. Concepts and definitions

1. VIRTUAL CURRENCIES

Virtual currencies are not a new concept, with multiple virtual currencies having come and gone over the past decade, starting from E-Gold (1996), WebMoney (1998), Liberty Reserve (2006), Bitcoin (2009) etc.[1]

Despite this fact, there is no unified definition on virtual currencies at the moment. Different agencies and institutions are providing different definitions regarding their own understanding of the virtual currencies like European Central Bank[2], International Monetary Fund[3], World Bank[4], FATF[5] and other international institutions[6].

Within the European Union, virtual currencies are defined in Article 1, 2), d) of 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 purpose of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU[7]. Thus, virtual currency is "a digital representation of value which is not issued or guaranteed by a central

1 Basic Manual on Detection and Investigating of the Laundering of Crime Proceeds using Virtual Currencies – UNDOC, June 2014 pg.7 and 8 **https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf**

2 European Central Bank "Virtual Currency Schemes", October 2012, **https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf**

3 International Monetary Fund Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, **https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf**

4 Distributed Ledger Technology (DLT) and Blockchain, FinTech Note no.1, World Bank Group, International Bank for Reconstruction and Development, 2017 - **https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf**

5 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, **http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf**, FATF Guidance for risk based approach Virtual Currencies, June 2015 **https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf** and FATF Guidance for a risk based approach, Virtual Assets and Virtual Assets Service Providers, June 2019 **https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf**

6 Such as The European Banking Authority, The European Securities and Markets Authority etc.

7 This Directive is also known as Fifth Anti Money Laundering Directive (AMLD5) **https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843&from=EN**

bank or a government, which is not necessarily linked to a legally determined currency and which does not have the legal status of currency or money, but which is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."

The given definition refers to the common characteristics of the virtual currencies:

1. VC are digital representation of value
   The value in general can be represented in the physical world (e.g. gold, real estate, real money) as well as in the digital world (electronic money, virtual currencies). Unlike the value in the physical world, the value in the digital world is virtual, meaning that is not tangible, is immaterial and consists purely of information.
2. VC can be transferred, stored and traded electronically
3. VC are not issued or guaranteed by a central bank or a government and do not have the legal status of currency or money
   Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency – i.e. it electronically transfers value that has legal tender status.[8] Here, it should also be noted that the term "digital currency" has a wider scope than the term "virtual currency" since it means digital representation of either virtual currency as a non-fiat currency or e-money as a fiat currency.
4. VC are not necessarily linked to a legally determined currency
5. VC are accepted by natural or legal persons as a means of exchange
   This aspect justifies the term "currencies". Despite the fact that virtual currencies are not money, since they do not involve a claim on a bank or government, they are accepted by their users as a medium of exchange and can also be a unit of account and a store of value.

Unlike the definition given in the AMLD5, in its latest recommendations FATF has adopted broader approach, accepting the concept of **„virtual assets"** instead of the concept of "virtual currencies". The main reasons for widening the definition of virtual currencies and introducing the concept of virtual assets are 1) the development of new technologies that enable or allow for reduced transparency and increased obfuscation of financial flows, 2) the emergence of other virtual asset business models or activities that present risk from criminal point of view

8 Basic Manual on Detection and Investigating of the Laundering of Crime Proceeds using Virtual Currencies – UNDOC, June 2014, pg. 4

and 3) the emergence of new illicit financing typologies, including the increasing use of virtual-to-virtual layering schemes that attempt to further obfuscate transactions in a comparatively easy, cheap, and secure manner.[9] Virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.[10]

The first observation is that the AMLD5 definition of "virtual currencies" is a lot narrower than the FATF definition of "virtual assets".[11] It only covers the virtual currencies and does not encompass other types of crypto-assets, most notably tokens.

Regardless of the term used, there are two main sub-types of virtual currencies: a) convertible and non-convertible virtual currency and b) centralized and decentralized virtual currency.

1.1. Convertible and non-convertible virtual currency

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency. Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney.[12] It should be emphasized that the notion of "convertible currency" does not in any way imply an ex officio convertibility (e.g. in the case of gold standard), but rather a de facto convertibility (e.g. because a market exists). Thus, a virtual currency is "convertible" only as long as some private participants make offers and others accept them, since the "convertibility" is not guaranteed at all by law.[13]

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon.com, and under the rules governing its use,

9 FATF Guidance for Risk-based Approach to Virtual Assets and Virtual Asset Service Providers, June 2019 pg. 6 **https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf**

10 Ibid. pg. 57

11 R. HOUBEN and A. SNYERS, "Crypto-assets, Key developments, regulatory concerns and responses", European Parliament Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies study, April 2020, pg.48 (electronically available via **https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf)**.

12 Basic Manual on Detection and Investigating of the Laundering of Crime Proceeds using Virtual Currencies – UNDOC, June 2014, pg. 4 and 5

13 FATF Guidance for a Risk-based Approach to Virtual Currencies, June 2015, pg.27

cannot be exchanged for fiat currency. Examples include: Project Entropia Dollars; Q Coins; and World of Warcraft Gold.[14] It should be noted that a non-convertible characterization is not necessarily static, since even where, under the terms set by the administrator, a non-convertible currency is officially transferrable only within a specific virtual environment and is not convertible, it is possible that an unofficial, secondary black market may arise that provides an opportunity to exchange the "non-convertible" virtual currency for fiat currency or another virtual currency. Generally, the administrator will apply sanctions (including termination of membership and/or forfeiture of remaining virtual currency) to those seeking to create or use a secondary market, contrary to the rules of the currency. Development of a robust secondary black market in a particular "non-convertible" virtual currency may, as a practical matter, effectively transform it into a convertible virtual currency.[15]

1.2. Centralized and decentralized virtual currency

Centralized Virtual Currencies have a single administrating authority (administrator)—i.e. a third party that controls the system. An administrator issues the currency, establishes the rules for its use, maintains a central payment ledger and has authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible virtual currency may be either floating— i.e. determined by market supply and demand for the virtual currency – or pegged— i.e. fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payments transactions involve centralized virtual currencies. Examples: E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life "Linden dollars"; PerfectMoney; WebMoney "WM units"; and World of Warcraft gold.[16]

Central bank digital currencies (CBDC) are digital currencies that are issued by central banks, thus they are virtual form of fiat currency. A CBDC is an electronic record or digital token of a country's official currency and as such is backed by the full faith and credit of the issuing government.[17] CBDCs can be designed in a number of ways, thus there is no single definition of what constitutes a CBDC. At the most basic level, a CBDC can be described as "monetary value stored electronically that represents a liability of the central bank and can be used

14 Basic Manual on Detection and Investigating of the Laundering of Crime Proceeds using Virtual Currencies – UNDOC, June 2014, pg. 4 and 5

15 FATF Guidance for a Risk-based Approach to Virtual Currencies, June 2015, pg.27

16 Basic Manual on Detection and Investigating of the Laundering of Crime Proceeds using Virtual Currencies – UNDOC, June 2014, pg. 5

17 **https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp**

to make payments". However, CBDCs should not be mistaken for crypto-assets, since a) whereas crypto-assets are private assets, CBDCs are sovereign in nature and b) whereas the issuance of crypto-assets relies on the use of DLT or similar technology, the issuance of CBDCs is not contingent upon the use of any specific technology.[18]

Decentralized Virtual Currencies (a.k.a. crypto-currencies) are distributed, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight. Examples: Bitcoin; LiteCoin; and Ripple.[19] Cryptocurrency refers to a math-based, decentralized convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralized, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the "block reward" and in some cases, also transaction fees paid by users as an incentive for miners to include their transactions in the next block).[20]

In practice, most of the virtual currencies appearing in criminal proceedings are crypto-currencies.

2. VIRTUAL CURRENCY SYSTEM PARTICIPANTS

2.1. Coin inventors and administrators/issuers

Coin inventors are individuals or organizations who create virtual currency and develop the technical part of the network.[21] In some cases their identity is known (e.g. Ripple, Litecoin, Cardano), but ever so often they remain unidentified

18 "Crypto-assets, Key developments, regulatory concerns and responses", Prof. Dr. Robby Houben and Alexander Snyers, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, European Parliament, April 2020 pg.27

19 Basic Manual on Detection and Investigating of the Laundering of Crime Proceeds using Virtual Currencies – UNDOC, June 2014, pg. 5

20 FATF Guidance for a Risk-based Approach to Virtual Currencies, June 2015, pg.27 and 28

21 ECB, "Virtual Currency Schemes – a further analysis", February 2015, pg.7 **https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf**

(e.g. Bitcoin, Monero).[22] Some remain involved in maintaining and improving the cryptocurrency's code and underlying algorithm (in principle without administrator's powers), whilst others simply disappear (e.g. Bitcoin).[23]

Issuers are able to generate units of the virtual currency. Depending on the design of the VC, the total issuance volume is predetermined or depends on demand. In centralized virtual currencies issuers are often the administrator of the VC[24]. An administrator is a person or entity engaged as a business in issuing (putting into circulation) a centralized virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to redeem (withdraw from circulation) the virtual currency.

2.2. Mining and miners

Mining is a process of creating new VC by solving complicated mathematical problems using high-performance computers. The result of the mining is twofold. First, when computers solve these complex math problems on the virtual currency network, they produce new VC. And second, by solving computational math problems, the transaction information is being verified, thus enabling trustworthy and secure network. Transaction is the movement of the VC from one account to another, so in the process of mining verification of the previous transaction history is being done by verifying how the VC has arrived at the public address now making the transfer. The transactions are clumped together in "blocks" and added to a public record called a blockchain.[25]

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. It is a type of database, where information is gathered in groups, also known as blocks. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. Blocks have certain storage capacities and, when filled, are chained onto the previously filled block, forming a chain of data – hence the name "blockchain".[26]

---

22 R. HOUBEN and A. SNYERS, "Crypto currencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion", European Parliament Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies study, July 2018, pg.28 (electronically available via **https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU-(2020)648779_EN.pdf)**

23 ECB, "Virtual Currency Schemes – a further analysis", February 2015, pg.7 **https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf**

24 Ibid.

25 **https://www.investopedia.com/terms/b/bitcoin-mining.asp**

26 **https://cointelegraph.com/bitcoin-for-beginners/how-does-blockchain-work-a-beginners-guide-to-blockchain-technology**

However, blockchain technology can be used on much wider scale. With its ability to create more transparency and fairness while also saving businesses time and money, the technology is impacting a variety of sectors in ways that range from how contracts are enforced to making government work more efficiently.[27] Few examples of such use are in following fields: money transfer and payment processing, supply chains monitoring, retail programs based on loyalty rewards, digital IDs, sharing of data, protection of loyalty and copyright, digital voting, transfer of real estate, food safety and unchangeable data backup.[28]

The entities performing the mining process are known as miners. A **miner** is an individual or entity that participates in a decentralized virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system[29] used to validate transactions in the virtual currency system.[30] When VC miners add a new block of transactions to the blockchain, part of their job is to make sure that those transactions are accurate. In particular, VC miners make sure that VC is not duplicated, a unique quirk of digital currencies called double-spending.

Transactions of virtual currencies are technically different from bank transactions and do not produce the same sets of data that bank transactions produce. Virtual currencies are transferred from one public address (that of a payer) to another (that of a service provider) and this transaction, after being validated, is included in the blockchain.

Each transaction exists of:

1. A transaction ID (hash value)
2. The number of VC that were sent
3. A transaction fee
4. One or more transaction inputs (aka UTXO's)[31] or address(es) of the sender
5. One or more transaction outputs (one or more receiver addresses and possibly one or more change addresses).[32]

27 **https://builtin.com/blockchain/blockchain-applications**

28 **https://www.analyticsinsight.net/real-world-applications-of-blockchain-technologies/**

29 Ethereum has developed a proof of stake system instead proof of work - **https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/**

30 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, pg. 7 and 8 **https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf**

31 UTXO: Unspent Transaction Output. More info at: **https://en.wikipedia.org/wiki/Unspent_transaction_output**

32 "Guide on seizing cryptocurrencies", Cybercrime program office of Council of Europe, February 2021, pg.13

2.3. User

A user is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. [33]

Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralized virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) with some decentralized virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them, and receive them as gifts, rewards, or as part of a free initial distribution.[34] Thus, miners may be also users, if they self-generate a convertible virtual currency solely for their own purposes, e.g. to hold for investment or to use to pay an existing obligation or to purchase goods and services.

2.4. Exchanger

An exchanger (also sometimes called a virtual currency exchange) is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.[35]

Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency.

It should be noted that there is a difference between **exchanges** which are marketplaces where users can find each other to exchange VC for traditional money or other VC and vice versa and **exchangers**. There are many differences in the technology and financial issues between exchanges and exchangers. But the main distinction between them is the fact that when referring to an exchanger, you conduct trading operations with it, while on the exchange you buy and sell

33 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, pg. 7 and 8 **https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf**

34 Ibid.

35 Ibid.

cryptocurrency, not from the exchange itself (which only provides access to the trading market), but by working with the private owners of the cryptocurrency and fiat assets.[36]

The main purpose of cryptocurrency exchanges is playing on the price of the asset, not the exchange operation of one coin to another. We are talking about trading signals, offering your asset prices. Cryptocurrency exchanges must be licensed in the countries they work and such detailed customer data is requirement for regulators.[37] Most of these services require you to go through the full registration, including passport details, home address, and more. In some exchangers, you are not required to register. In these cases the exchanger is not interested in your workplace and your real name — it is just a quick and easy option to buy or sell the cryptocurrency. [38]

As it was mentioned earlier in this Handbook, attempting to widen the scope of existent definitions and to adjust them to new and future technological developments, FATF adopted a definition on virtual assets and, consequently, on **virtual asset service provider**. Thus, a virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

a. exchange between virtual assets and fiat currencies;
b. exchange between one or more forms of virtual assets;
c. transfer of virtual assets;
d. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
e. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

In this context of virtual assets, transfer means - to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.[39]

It is clear that, in light of the above given definition, exchanges are considered virtual service providers and thus are obliged by FATF Recommendations. From a criminal investigation point of view, the data and records that exchanges, as virtual asset providers, are obliged to hold and keep under FATF Recommendations, can prove to be valuable investigative tool for the law enforcement authorities.

---

36 **https://cryptocurrencyhub.io/exchanger-vs-exchange-which-one-to-choose-73af890dea0a**

37 For example Coinbase (CB Payments Ltd.) is registered in the UK

38 **https://cryptocurrencyhub.io/exchanger-vs-exchange-which-one-to-choose-73af890dea0a**

39 FATF Guidance for Risk-based Approach to Virtual Assets and Virtual Asset Service Providers, June 2019 pg.57 **https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf**

2.5. Trading platforms

In addition to cryptocurrency exchanges, the so-called "trading platforms" also play an important role in the exchange of cryptocurrencies (and, most notably, allow cryptocurrency users to buy coins with cash).[40] Trading platforms function as marketplaces, bringing together buyers and sellers of virtual currencies by providing them with a platform on which they can offer and bid among themselves i.e. directly trade with each other. In contrast to exchanges, however, the trading platforms do not engage in the buying and selling themselves. Some trading platforms, such as www.localbitcoins.com, give their customers the option of locating potential customers nearby.[41]

2.6. Virtual currency wallet

Virtual currency wallet is a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency.[42] Some wallets are built for a single cryptocurrency, some can be used for more than one coin, some wallets you'll manage yourself, and some (like those found on exchanges) will be custodial.[43]

Each wallet type is a little bit different, but in general, any given wallet will work with one or more cryptocurrencies and will be able to store one or more cryptocurrency-specific "public addresses." Apart from public addresses, the VC wallet contains the public and private keys for each of the public addresses.

Public addresses (a.k.a. virtual currency addresses) are like virtual currency-specific account numbers; they can be used to receive a specific type of virtual currency (for example, to receive Bitcoin, you need a Bitcoin address) and can be shared publicly. Each address relates back to all transactions associated with that address on a coin's blockchain. These addresses are known by all users of the blockchain and can be compared to a bank account number, although everyone can also consult the balance.[44] Public addresses are hash versions of the public keys.

---

40 R. HOUBEN and A. SNYERS, "Crypto currencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion", European Parliament Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies study, July 2018, pg.27 (electronically available via **https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf**).

41 ECB, "Virtual Currency Schemes – a further analysis", February 2015, pg.8 **https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf**

42 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, pg.7 **https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf**

43 **https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-wallet/**

44 The EJCN Virtual Currencies Guide for Judicial Authorities

The **public keys** are cryptographic codes that allow users to receive messages, coins, or tokens and are mainly used for dissemination. By sending these assets with a public key, they are converted into a different format—one that is unreadable by people who aren't intended to be receivers (ones that don't have the private key). These keys often come in the form of long strings of alphanumeric characters.[45] A public key is designed to identify the user and generate the user's virtual currency address, allowing users to receive messages, coins, or tokens. The public key is also mathematically irreversibly derived from your private key (irreversibly since using reverse mathematics to derive the private key from the public key would take the world's most powerful supercomputer many trillion years to crack).[46]

A private key is a code of letters, numbers and/or symbols used to initiate virtual currency transactions (transfers). The private key acts as a lock for a specific virtual currency address and is somewhat similar to a bank account password. The owner (or user) of this key has access to the virtual currency balance linked to a specific virtual currency address, so that the person in possession of the private key is free to transfer the virtual currency from the address to which the private key is linked to any other address. Since the private key grants the access to the virtual currency address, and allows virtual currencies to be spent, it is crucial to never lose or disclose the private key to anyone. The person holding the private key has the virtual currencies at his disposal.[47]

In essence, the private key decrypts the content of the public key, enabling the holder of the private key to access the decrypted content. Thus, proving you own the address is done with a private key in non-custodial wallets. In custodial wallets, the custodian (a third party like an exchange, broker, etc.) holds the key for you, and it is just a matter of inputting your password into their wallet app.[48]

A wallet comes with an address by default, which is different from the public addresses, described above.[49] The wallet lets you view balances associated with an address and lets you move funds around on the blockchain as long as you are the owner of the address.

A cryptocurrency wallet can consist of a string of different public addresses. The fact that it's called "a wallet" can be a little misleading because it doesn't actually hold all your credit cards in the way that Apple Pay does, for example.

45 **https://paxful.com/blog/what-are-public-keys-private-keys-wallet-address/**

46 Ibid.

47 The EJCN Virtual Currencies Guide for Judicial Authorities

48 **https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-wallet/**

49 For more information you can consult **https://medium.com/hackernoon/crypto-wallet-vs-address-54f7fb980bd3**

Instead, a cryptocurrency wallet is more similar to a key ring because it holds a copy of each private key and its corresponding address. So, regardless of whether you own just Bitcoin, or Ethereum, or a host of several different cryptocurrencies, all you need to do is open your wallet to gain access to all the different addresses contained within it.[50]

There are different ways you can access your cryptocurrency wallet: on a desktop, on a browser, or by using a physical wallet. Otherwise known as "cold storage," physical wallets are more secure because they're offline and less susceptible to hacks. Web and Mobile/Desktop wallets are also called "online" or "hot" wallets.

A **web wallet** means that access to the VC (private key - public address) is kept online with a service provider. The advantage is that this VC is immediately available to the user. The disadvantage is that if someone gains illegal access to the system of the service provider, he/she also has access to the VC. In addition, there is also a chance that a rogue service provider will embezzle the VC of the customers.[51] A specific type of web wallet is the dark wallet, which is a browser-based extension wallet that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymizer (mixer); decentralized trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralized market places.[52]

A **Mobile or Desktop wallet** user's that access to the VC (private key - public address) is stored on the user›s system (smartphone / tablet or desktop PC, respectively) via an application or program whether or not protected by a password.[53]

A physical wallets means that access to the VC is not available online. This has the advantage that the VC is safe for possible hackers, but in turn entails an increased risk of loss if the physical carrier on which these keys are stored is lost or stolen. An example of such a system is a **hardware wallet**, where the private keys are on a separate device.[54]

There is also a **paper wallet**, where the public address and the private key are available on a paper carrier. This medium can clearly be easily copied, so that anyone who has it can access the VC at the public address in question.

50 **https://thenextweb.com/news/the-differences-between-a-bitcoin-wallet-and-an-address**

51 The EJCN Virtual Currencies Guide for Judicial Authorities

52 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, pg. 7 **https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf**

53 Ibid.

54 Ibid.

Sometimes, however, the private key is printed encrypted. In that case, the private key must first be made readable with a separate key.[55]

Knowing the type of wallet in question will determine how the access to the VC can be gained. Here it should be noted that the private key, discussed above, is not used to access the wallet, but to access a virtual currency address that is stored in the wallet.

2.7. Wallet provider

A wallet provider is an entity that provides a virtual currency wallet (i.e. a means - software application or other mechanism/medium for holding, storing and transferring bitcoins or other virtual currency).[56] Simply put, a wallet holds a virtual currency user's private keys. A wallet provider typically translates a virtual currency user's transaction history into an easily readable format, which looks much like a regular bank account.[57] It also maintains the user's virtual currency balance and generally provides storage and transaction security.[58]

Having in mind that there are different types of wallets, as explained above, in reality, there are several types of wallet providers:

- Hardware wallet providers that provide cryptocurrency users with specific hardware solutions to privately store their cryptographic keys (e.g. Ledger Wallet, ...);
- Software wallet providers that provide cryptocurrency users with software applications which allow them to access the network, send and receive coins and locally save their cryptographic keys (e.g. Jaxx);
- Custodian wallet providers that take (online) custody of a cryptocurrency user's cryptographic keys (e.g. Coinbase).[59]

---

55 Ibid.

56 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, pg. 7 and 8 **https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf**

57 R. HOUBEN and A. SNYERS, "Crypto currencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion", European Parliament Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies study, July 2018, pg.27 (electronically available via **https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf**).

58 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, pg. 7 and 8 **https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf**.

59 R. HOUBEN and A. SNYERS, "Crypto currencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion", European Parliament Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies study, July 2018, pg.27 (electronically available via **https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf**).

Wallet providers, as exchanges, fall under the FATF definition for virtual service providers.

2.8. Seed

In virtual currencies, a recovery seed, or shortly seed, is a list of words in a specific order which store all the information needed to recover a virtual currency wallet. Usually, the seed is a list of words generated at random, usually consisting of between 10 and 24 words. With the recovery seed you can access the wallet and recover private and public keys found in the wallet. Keeping the recovery seed private and safe is key for long-term safety of the user›s virtual currency funds. Thus, the seed can be stored in a written or printed form or in different type of electronic files (text, pdf, picture) on the user's computer or electronic device.[60]

2.9. Payment providers

Payment providers offer the possibility to pay with VC to purchase products or they could provide the service to convert the VC in another currency and then transfer the payment to the (online) seller. They very often keep all the data involved.[61]

Payment providers, same as exchanges and wallet providers, fall under the FATF definition for virtual service providers.

2.10. Anonymizer (anonymizing tool)

Anonymizer refers to tools and services, such as darknets and mixers, designed to obscure the source of a VC transaction and facilitate anonymity. (Examples: Tor (darknet); dark wallet (darknet); Bitcoin Laundry (mixer)).[62]

2.11. Mixers and tumblers

Due to blockchain technology, cryptocurrencies feature a publicly visible register of all transactions where all cashflows are traceable. Mixers and tumblers are designed to increase anonymity and allow users to re-establish their financial privacy when using cryptocurrencies.

A mixer (or tumbler) is any service that mixes cryptocurrency assets and tokens to obscure their traceable origin. The cryptocurrency owner transfers the money

60 The EJCN Virtual Currencies Guide for Judicial Authorities

61 The EJCN Virtual Currencies Guide for Judicial Authorities

62 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, pg. 6

to the mixing service, which mixes it with that of other users and transfers the mixed currency to the desired address, meaning there is no connection between the original transaction and this address.

A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed. (Examples: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).[63]

There are different types of solutions when it comes to mixers. Centralized mixers are privately owned services that accept your coin and send back different coins for a fee.[64] If many people use a particular mixing service, it becomes increasingly difficult for an outsider to tie any of the "incoming" coins to any of the "outgoing" coins. This breaks the transaction trail, offering privacy to the users.[65]

Centralized mixers have access to your Bitcoin and IP addresses. They ultimately know which address sent and received which coins and are keeping logs and data. From a law enforcement perspective, information like these can be requested from a mixer.[66] However, it should be noted that some centralized mixer platforms like BitcoinMix.org do not store logs or collect personal data about the user and are completely automated.

Decentralized mixers are peer-to-peer mixing services available on more advanced blockchain platforms. These mixers attempt to fix the shortcomings of centralized mixing. Individuals band together and pool their coins to make one significant transaction, and the coins get randomly returned to the pool members. The higher the number of users in the pool, the higher the randomization. The most popular non-custodial mixers include Wasabi Wallet and Samourai Whirlpool.[67] The protocol most common in this decentralized mix

63 Ibid.

64 **https://en.cryptonomist.ch/2020/08/15/bitcoin-mixers-centralized-decentralized/**

65 **https://bitcoinmagazine.com/guides/what-are-bitcoin-mixers**

66 All interactions done thru mixer platform can be obtained by the law enforcement agencies like IP-addresses, transaction details, bitcoin addresses and chat messages. Such an example was the clamping down on one of the world's leading cryptocurrency mixing service Bestmixer.io. More on: **https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down**
It should be noted that in US mixer can be held accountable for enabling money laundering. Such example is the case of Helix mixer. More on: **https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million**

67 Non-custodial mixers are user-hosted software tools, not third-party services that take custody of user funds, where the mixer services are part of the wallet.

is known as CoinJoin. CoinJoin aims to improve privacy by coordinating inputs of multiple users into a single transaction. The transaction gets multiple outputs that obscure the origins of the coins. However, some CoinJoins have easily recognizable patterns on the blockchain and Blockchain analysis services can de-anonymize a sender who used CoinJoin.[68]

2.12. Tor

Tor, short for "The Onion Router" is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network. This difficulty can be exacerbated by use of additional tumblers or anonymizers on the Tor network. Tor is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated internet activity.[69]

2.13. VPN

A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.[70]

2.14. Bitcoin

Bitcoin was the first decentralized convertible virtual currency and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into any fiat or virtual currency.[71]

---

68 **https://en.cryptonomist.ch/2020/08/15/bitcoin-mixers-centralized-decentralized/**

69 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, pg. 6

70 **https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html**

71 FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, pg. 5 and 6 **https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf**

2.15. Altcoin

Altcoins (alternative coins) is a term used to describe all math-based decentralized convertible virtual currency other than Bitcoin. Their name comes from the fact that they›re alternatives to Bitcoin and traditional fiat money. Depending on their functionalities and consensus mechanisms, altcoins can be sorted in various categories. It should be noted that it is possible for an altcoin to fall into more than one category. The main types of altcoins include mining-based cryptocurrencies, stablecoins, security tokens, and utility tokens. [72]

It should be noted that there is a distinction between cryptocurrencies and tokens. Tokens are those crypto-assets that offer their holders certain economic and/or governance and/or utility/consumption rights. Broadly speaking, they are digital representations of interests, or rights to (access) certain assets, products or services. Tokens are typically issued on an existing platform or blockchain to raise capital for new entrepreneurial projects, or to fund start-ups or the development of new (technologically) innovative services. [73]

2.15.1 Mining-Based cryptocurrencies

As their name indicates, mining-based altcoins are mined into existence. Miners solve complex mathematical puzzles to verify transactions, create blocks, and mine new coins simultaneously. Most mining-based altcoins use Proof-of-Work (PoW), a method in which systems generate new coins by solving difficult problems, to create blocks. The top list of mining-based Altcoins are Litecoin (LTC), Monero (XMR), Ethereum Classic (ETC), and DASH. [74]

The alternative to mining-based altcoins is pre-mined coins. Such coins are not produced through an algorithm but are distributed before they are listed in cryptocurrency markets. An example of a pre-mined coin is Ripple's XRP.

2.15.2 Stablecoins

Stable coins are coins that are pegged to a basket of goods, such as fiat currencies, precious metals, exchange-traded commodities, securities or other cryptocurrencies. This basket is meant to act as a reserve to redeem holders if the cryptocurrency fails or faces problems.

Stablecoins have low price volatility, since their value is dependent on real-life assets and the price fluctuations for stablecoins are not meant to exceed a

72 **https://www.investopedia.com/terms/a/altcoin.asp**

73 "Crypto-assets, Key developments, regulatory concerns and responses", Prof. Dr. Robby Houben and Alexander Snyers, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, European Parliament, April 2020 pg.18

74 **https://www.investopedia.com/terms/a/altcoin.asp**

narrow range. Thus these coins assure stability in terms of price, which makes them a perfect option for cryptocurrency trading.

While Tether (USDT) is the most widely used stablecoin, other alternative coins in this category are USDCoin (USDC), Maker (MKR), and DAI.

2.15.3. Security tokens

Security tokens are similar to securities traded in stock markets except they have a digital provenance. These alternative coins act as digital financial securities that investors can receive through initial coin offerings (ICOs). By investing in them, token holders enjoy voting rights, dividends, market appreciation, and part ownership in the company. It should be noted that these digital coins fully comply with government regulations. Thus, having in mind the prospect of price appreciation for such tokens and their characteristics, institutional investors trust and invest in these tokens.

Examples of security tokens include ASPD, EXOD, OSTKO and TZROP.

2.15.4 Utility tokens

These alternative coins are not for investment purposes but allow token holders to purchase products and services or redeem rewards within a platform. Unlike security tokens, utility tokens do not pay out dividends or part with an ownership stake but give the users the right to vote and offer feedback on products they use while participating in the concerned blockchain ecosystem. Filecoin, which is used to purchase storage space on a network, is an example of a utility token.

3. How the concept of virtual currencies is put in practice

There are many guidelines and graphics that explain in detail the technical aspect of how the concept of virtual currencies is put in practice.[75]

However, having in mind the focus of this handbook we will further focus on their role in criminal proceedings only.

75 Such example is given in the graphic and you could read more in FATF Guidance on Risk Based Approach on Virtual Currencies June 2015 pg.39 **https://thumbnails-visually.netdna-ssl.com/bitcoin-infographic_5029189c9cbaf.jpg**

III. Importance of virtual currencies in criminal proceedings

From a view point of criminal proceedings the virtual currencies can be instrumentalities of a crime, they can be proceeds of a crime and can be used as evidence.[76] In any of these cases, law enforcement authorities first must detect and then secure the virtual currencies. Consequently, the law enforcement authorities need to have specific knowledge and understanding on the process of detecting and later obtaining control over VC.

Access to VC and control over it presupposes that one has a public key/address and the corresponding private key. Once you have this, you can deprive a suspect of the VC. A deprivation is only complete when the VC has actually been transferred to another address, which is not under the control of the suspect or his accomplices.[77]

1. DETECTING VIRTUAL CURRENCIES IN CRIMINAL PROCEEDINGS AND OBTAINING RELEVANT INFORMATION AND EVIDENCE

Detecting the presence and use of virtual currencies in criminal proceedings is the first step law enforcement authorities need to do. But the main question is what specifically to search for?

Having in mind how the technology behind virtual currencies works, **mining equipment, virtual currency addresses/public keys**, as well as **private keys** and **seed word lists** are of interest to the law enforcement authorities. When it comes to public address, it should be noted that they can also be consulted at any time via open sourcing.

As explained above, private and the public keys/addresses can be found in a person's virtual currency **wallet**. Having this in mind, one of the key information

76 E.g. As explained in the previous chapter, there are VC that work on blockchain technology. This technology contains lot of information that in the criminal proceedings can be used as evidence (e.g. information regarding previous transactions).

77 The EJCN Virtual Currencies Guide for Judicial Authorities

the investigation should aim to detect is the possible appearance of a wallet. Also, it should be noted that some wallets might be protected by PINs, so apart from the wallet, search for **passwords and PINs** is also a necessity. **QR codes** where passwords might be stored must not be overlooked.

There are different investigative activities that can be performed in order to find the necessary evidence like searches (house/premises, body or computer system search), questioning of the suspect and witnesses or doing online investigations.

Prior to conducting any investigative activities, proper investigative planning needs to be done and investigative strategy needs to be developed. For example, passwords or PINs can be found on different places such as under a keyboard, on a piece of paper, in an agenda, etc., thus it is important to obtain search warrant that will enable seizing of the passwords, PINs etc. together with the medium they are stored on.

Access to cryptocurrencies through (a) private key(s) or a seed phrase can be found locally e.g. on a desktop computer (i.e., a non-custodial wallet such as Electrum) or can be stored somewhere online on a custodial wallet in the same or another jurisdiction.[78] Thus, since wallets appear in different forms, it is necessary for the law enforcement to be able to recognize the type of wallet in question. The type of the wallet will influence on the decision what investigative activity needs to be performed in a concrete case.[79] Thus it can happen that the initial search in a criminal proceeding provides information about the existence and type of wallet and additional investigative activities might follow on basis of this information. Sometimes, indications of which virtual currencies a suspect is using can be obtained beforehand through an already initiated investigation. In this light it is essential that good communication is established between all law enforcement participants in order to avoid or diminish the possibility of destroying evidence or moving of the virtual currencies before they are officially seized.

Relevant information regarding the virtual currencies in one criminal proceeding can be obtained from an exchanger. The exchangers could be

78 "Guide on seizing cryptocurrencies", Cybercrime program office of Council of Europe, February 2021,pg.21

79 The EJCN Virtual Currencies Guide for Judicial Authorities contains a graphic outline of the investigative activities that can be done depending on the type of wallet and depending on the fact whether the wallet is on the device of the target or not on the device of the target, taking into consideration whether the device is offline or online. For example, in case where a mobile wallet is found on the mobile phone of the suspect and the mobile phone is online, available investigative activities are computer search as well as network search. However, if a paper wallet is found that is not on any device of the target and is not stored online, then seizure is the appropriate investigative activity for obtaining this wallet

storing: name; basic subscriber information, including IP-address; verified contact details; activity logs; IP logs; VC addresses; personal messages; payment information; a proof of ID, home address (passport, national IC, driver's license...) etc. They could also freeze/seize the VC on request.[80] However, the difficulty here is that the exchangers are located usually in foreign jurisdictions, so for obtaining information there might be a need to draft MLA request. It should be noted that in some cases, the exchangers directly voluntarily cooperate with law enforcement authorities.[81] It should also be noted that cooperation should be established only with trusted exchangers. Exchangers are often used for money laundering, sometimes are a scam at itself or that they have a policy that they warn their customer that law enforcement is asking questions. Thus, it is necessary to be very well informed (by your specialized police unit or Europol) before giving the order to approach the exchanger.[82] It should be noted that Europol has published a list of contacts on cryptocurrency exchanges and other compliant entities and that this list is available for law enforcement and judiciary entities.

The EJCN Virtual Currencies Guide for Judicial Authorities provides practical example on what information can be requested from an exchanger. Thus, it is strongly recommended that this guide is also consulted when dealing with virtual currencies in criminal proceedings.

Annex I of this Handbook provides a template of a request for service provider data detailing types of information that can be obtained from an exchanger.

Also, there are physical exit points that provide VC cashing or trading services. Not only the provider could be requested for available information about a certain transaction or a certain VC address, it could also offer the investigative opportunity to search for physical evidence surrounding the physical exit point (cash/trading machine), such as CCTV evidence in the neighborhood of or pointed at the exit point. A global oversight of available exit point can be found on **https://coinatmradar.com**.[83]

80 The EJCN Virtual Currencies Guide for Judicial Authorities

81 Some cryptocurrency exchanges, like Binance, have provided forms for asking assistance (information requests) by law enforcement authorities - **https://www.binance.com/en/support/law-enforcement**

82 The EJCN Virtual Currencies Guide for Judicial Authorities

83 The EJCN Virtual Currencies Guide for Judicial Authorities

Law enforcement authorities should keep in mind that under AMLD5[84] users that hold their virtual currencies via a custodian wallet provider or enter into virtual currency transactions via a virtual exchange platform can no longer be anonymous, because of the customer due diligence requirements vested upon the custodian wallet providers and virtual currency exchange platforms. Thus, in some cases relevant evidence can be found there.[85] However, no evidence in this light can be found on the trading platforms, since they are not run by an entity or company that oversees and processes all trades, but they are operated exclusively by software (i.e. there is no central point of authority).

2. OBTAINING CONTROL OVER VIRTUAL CURRENCIES

The information gathered during the investigation and discussed in the previous chapter is essential for law enforcement authorities to be able to obtain control over VC. For successful seizure of VC several steps are identified[86]:

1. Identify (locate) VC
   Identification of VC includes the obtaining information about the type VC in question, their quantity and the possibility to access the VC..
2. Identify a link between VC and the user
   This has proven to be the hardest part of the investigation. Though there are some activities that might help in establishing the link between the VC and the user[87], in most cases, this link can be established on the basis of the evidence and facts found during searches.
3. Ensure access to the VC
   This can be done either by obtaining the accesses from the suspects/users[88] or by identifying the wallets, obtaining private keys and passwords

84 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

85 No such evidence should be expected from VC exchangers that accepts only cryptocurrency and in cases when anonymous cryptocurrencies were used

86 EJCN Virtual Currencies Guide for Judicial Authorities

87 As the EJCN Virtual Currencies Guide for Judicial Authorities points out, this can be done with the use of the "follow the money" approach when analyzing transactions that are normally public and verifiable, through the inspection of public ledgers or blocks (e.g. using Chainalysis software). Since users of virtual currencies are anonymous, the purpose of this approach is to uncover the identity of an unknown perpetrator or to link a known perpetrator to illegal proceeds, which can be achieved by identifying the provider of the perpetrator's electronic wallet; identifying the IP address of the user of a particular electronic wallet, and acquiring the data on the perpetrator's trading account with the provider of an online exchange.

88 It should not be excluded that the suspect/users would like to voluntarily provide access to the law enforcement authorities. If during suspect questioning the suspect admits the use of wallet and provides written consent to the seizure of the VC by means of his computer system, the police can do so immediately in accordance with article 32 b) of the Budapest Convention on Cybercrime without any further procedural requirements. However, in some jurisdictions, it will be possible to force suspects to hand over certain passwords (encryption keys, private keys).

for recovery of private keys[89]. Without ensuring access to the VC, they cannot be secured.

4. Obtain legal instrument for seizure
   Seizure is possible only if legal grounds exist and only if a proper legal instrument for seizure is being issued by the competent authority.
5. Enforcing the seizure
   After legal instrument for seizure has been obtained, the seizure must be enforced. There are two main possibilities for enforcing the seizure: a. to store and secure the VC (this is done by transferring the VC from the user's wallet to a secure wallet controlled by the law enforcement authorities) and b. convert the seized VC (this is done by selling the VC).

As mentioned, securing of VC is done by transferring the VC form the user's wallet to a secure - government controlled wallet. A government-controlled wallet is a wallet under control of the government or state. More particularly, depending on the legal framework, this wallet can be under control of a law enforcement agency, a Court, an (investigative) judge, a public prosecutor, a confiscation body, a private company dealing with asset management, or even an auction house.[90]

If applicable (i.e. taking into consideration the corresponding legal framework and seizing procedures), it is a good practice to prepare the proper seizing address(es)[91] and government-controlled wallet(s) in advance as soon as there is a chance to be confronted with a virtual currency seizure. Depending on which cryptocurrencies are to be found, there could be a necessity to prepare several government-controlled wallets such as one for Bitcoin, another one for Monero and so on or, instead of these different wallets, a multi-currency wallet can be used. Thus, if applicable, the creation of these addresses/wallets must be done in a safe computer environment and strongly recommended having a written step-by-step guide as a projection of the internal rules. It is advised to use a single address for every suspect seizure or confiscation.[92]

Depending on which government-controlled wallet and/or procedure will be used, an option could be to have prepared in advance the seizing address as a QR code to avoid typos. Right before executing a seizure, this seizing address needs to be double-checked to see if the address is still correct. A suggestion

89 This information can be found on the grounds of examination of digital data, stored on electronic or associated devices.

90 "Guide on seizing cryptocurrencies", Cybercrime program office of Council of Europe, February 2021, pg.23

91 The seizing address is the address where the seized cryptocurrencies will be sent to

92 "Guide on seizing cryptocurrencies", Cybercrime program office of Council of Europe, February 2021, pg. 24

hereby is to use the four-eyes principle in which four eyes can check the correctness of the seizing address and hence safeguard the persons who are seizing the assets.[93]

One other point that needs to be taken into consideration in the seizure of virtual currencies are the transition fees. Namely, for transferring the VC to a secure wallet, a transaction fee needs to be paid. Thus, it is good practice to review this issue in advance, decide who will be paying the transaction fee and decide upon the amount of the transaction fees that will be paid.[94]

Even in cases when VC conversion is an option, it should be noted that this process will usually come after the VC are secured and transferred onto a government-controlled wallet. Also, it must be taken into account that the suspect might later be found innocent and the converted VC will have to be reimbursed to this individual.

93 "Guide on seizing cryptocurrencies", Cybercrime program office of Council of Europe, February 2021, pg.26

94 It should be taken into consideration that transaction fees can vary and that one can offer higher transaction fees for verifying certain transaction, gaining security that theirs transaction will have priority over other possible transactions on the same VC.

IV. North Macedonia legislation regarding virtual currencies

North Macedonia legislation does not recognize virtual currencies as such. At the moment of publishing of this Handbook no existent law defines or regulates the subject of virtual currencies. However, there are ongoing legislative and institutional analyses and attempts to address this topic.

The Financial Intelligence Unit of North Macedonia, as responsible national authority for implementing FATF Recommendations, has conducted a Risk assessment on the use of virtual assets for money laundering and financing of terrorism purposes. The Risk assessment is one of the few official documents that address the topic of virtual currencies from a ML/FT perspective.

Also, at the moment of publishing of the Handbook, the Ministry of Finance is working on a new Law for prevention of money laundering and financing of terrorism. One of the questions that this new law touches is the question of the virtual currencies. The draft proposal for the new law includes definitions on virtual assets; virtual assets provider; services or activities connected with virtual assets; storage and administration of virtual assets or instruments that enable control over virtual assets; organization of a virtual asset trading platform; execution of virtual asset orders on behalf of third parties; participation and provision of services related to the offer of the issuer and/or sale of virtual assets; virtual asset portfolio management; receiving and transmitting orders for virtual assets; publisher of virtual assets; public offering of virtual assets; providing advice on virtual assets; cryptomat; hosted electronic wallet for virtual assets; unhosted electronic wallet for virtual assets and virtual assets transactions. The definitions used in this draft law proposal are the ones used and defined by FATF.

Also, at the moment of publishing of this Handbook the Ministry of Justice is working on amendments and supplements to the Criminal Code and the Criminal Procedure Code of North Macedonia. In the working groups there is awareness about the need to define the virtual currencies and regulate their role in criminal proceedings, but at the moment of publishing of this handbook no official draft text has been adopted.

The Ministry of Justice is also working on the amendments to the Law on managing confiscated property, proceeds and seized objects in criminal and misdemeanor proceedings. In the draft proposal for this law the legislator

mentions the term "electronic money" and provides rules on how the Agency for confiscated assets will act in case where electronic money is temporary seized. In the section where definition of terms is given, no definition on what electronic money is considered is given. If we further analyze the legal solution, it can be concluded that the legal provision where electronic money is mentioned was intended to address the case of seizure and confiscation of virtual currencies and that the term "electronic money" is wrongly used. Having in mind that this is just a draft law proposal, there is enough time to make appropriate changes, that will involve use of correct terminology and that will include legal definition of terms.

The undergoing legal developments in North Macedonia will influence the way practitioners deal with virtual currencies in concrete cases. However, the existent legal grounds for confiscation and temporary safeguard measures will remain the same and the new solutions will provide form of an upgrade that will ease the work of the practitioners.

1. NATIONAL LEGAL GROUNDS FOR DEALING WITH VIRTUAL CURRENCIES IN CRIMINAL PROCEEDINGS

In relation to criminal proceedings, according to the current legislation there is a theoretical possibility in one criminal proceeding to seize and later confiscate virtual currencies if all the legal conditions are met. Key legislation that enables dealing with VC in criminal proceedings are the Criminal code of North Macedonia[95] and the Criminal Procedure Code of North Macedonia.[96] Relevant law that can help practitioners in the investigations and can be used in regard to virtual currencies is the Law on prevention on money laundering and financing on terrorism[97], as well as the Law on managing confiscated property, proceeds and seized objects in criminal and misdemeanor proceedings.[98] However, putting this theoretical possibility in practice is followed by practical difficulties.

95 Official Gazette of North Macedonia No 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 and 248/2018

96 Official Gazette of North Macedonia No.150/10, 100/12 and 198/18

97 Official Gazette of North Macedonia No. 120/18, 275/19 and 317/20

98 Official Gazette of North Macedonia no. 98/08, 145/10, 104/13, 187/13, 43/14, 160/14, 97/15, 148/15 and 64/18

1.1. Seizure and confiscation of virtual currencies as instrumentalities of crime

As mentioned, VC can be instrumentalities of crime. Article 100-a of the Criminal Code of North Macedonia provides that no person can keep or adopt the objects that have occurred through a commission of a crime. Objects that were intended or have been used to commit a crime shall be confiscated from the offender regardless of whether they belong to the offender or to a third party if this is in the interest of general safety, health of the people or moral reasons. Also, objects used or intended to be used to commit a crime may be confiscated if there is a threat that they may be used to commit another crime.

The definition of the term "objects" is also given in the Criminal Code[99], so objects shall include movable and immovable items being completely or partially used or should have been used or have resulted from a commission of crime. Thus, in cases where the VC appear to be instrumentalities of a crime (they occurred through a commission of a crime[100] or they were intended or have been used to commit a crime[101]) there is a possibility to seize and later confiscate the VC. The term "object" is widely defined, focusing only on the use or potential use of the objects, not the characteristics of the objects, so the legal provisions in the Criminal Code can be used as legal grounds for seizure and confiscation of VC that appear to be instrumentalities of crime.

When defining the term "money" the law mentions the term "electronic money". Thus, money shall be funds for paying cash, in denomination or in electronic money, which are considered as legal means of payment used in the Republic of North Macedonia or in a foreign country. Here it should be underlined that electronic money and virtual currencies are two different concepts. Electronic money is electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer[102]. Për rrjedhojë, ruhet lidhja ndërmjet parasë elektronike dhe formatit tradicional të parasë dhe ka një bazë ligjore, pasi mjetet e ruajtura shprehen në të njëjtën njësi të llogarisë (p.sh. dollarë amerikanë, euro, etj.).[103] This is not a case with virtual currencies, as explained in chapter II subchapter 1 of this Handbook.

99 Article 122 paragraph 39 of the CC

100 E.g. VC were mined for financing of terrorism purposes

101 E.g. VC used for money laundering purposes

102 Article 2 of the Directive 2009/110/ec of the European Parliament and of the Council of 16 September 2009 **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=en**

103 European Central Bank, Eurosystem, Virtual currency schemes, October 2012, page 16 **https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencymes201210en.pdf**

Prior to being able to seize the VC in criminal proceedings, the prosecutor should make sure that all conditions for obtaining control over VC are met.[104] The rules for seizure and later confiscation of the instrumentalities of crime are prescribed in the Criminal Procedure Code of North Macedonia.

1.1.1. Seizure of virtual currencies as instrumentalities of crime

According to the CPC[105] the instrumentalities of the crime can be temporary seized, confiscated or other temporary measure can be issued in order to prevent their use, transfer and managing. When it comes to VC it appears that seizure is the most appropriate temporary measure for their securing during the criminal proceeding, since the seizure will enable fulfilment of the purpose why temporary measure is being issued and will prevent the further use, transfer and managing of the VC.

Seizure of VC is done in all stages of the criminal proceedings, even in the pre-investigative stage. The general rule is that the seizure is done on grounds of a court ruling that is issued upon a request from the public prosecutor.

The prosecutor' request must contain all the mandatory elements that the CPC prescribes. In the cases of seizure of VC there are some distinguishing elements that the prosecutor must include in the seizure request. Thus, when drafting the VC seizure request, the prosecutor should make sure that the request includes:

- A short description of the criminal offence and its legal designation
- Description on the VC that originates or is related to the offence containing the type of the VC, the quantity/amount of VC and the location of the VC – the wallet identifier. The description of the VC should include the value of the VC at the moment of the request, since the court is obliged to point the value in the court ruling.
- Information on the user of the VC noting the name and surname of the user, his/her personal details
- Evidence on which the suspicion that the VC are instrumentalities of a crime is based
- Reasons for the probability that the seizure of the VC shall be made especially difficult or impossible until the end of the criminal proceedings. When describing these reasons, the practitioner should bear in mind that VC can be accessed remotely from different devices and that seizing one device without seizing the VC themselves is not sufficient.
- Propose the competent authority that will execute the seizure – this part is not mandatory but it can be useful, especially in cases where the

104 This was discussed in chapter III subchapter 2 of this Handbook

105 Article 202 from the CPC

prosecution office prefers other national authority, apart from the Agency for managing confiscated assets, to perform the seizure.
— Public address of a secure wallet where the VC will be transferred.

The request for seizure can be filed in the preliminary procedure or after the indictment has been filed. If the request is filed before the beginning and during the preliminary procedure, the preliminary procedure judge will be the competent authority that will deal with the request and if the request comes after the indictment has been filed, the Court will be the competent authority is the Court holding the hearing.

The procedure for seizure is urgent. The preliminary procedure judge shall rule immediately and no later than within 12 hours from the receipt of the request of the prosecutor. If the preliminary procedure judge does not accept the request by the public prosecutor, he/she shall ask the Trial Chamber of the criminal council within the Court to render a decision without any delay. The Trial Chamber shall render a decision within 24 hours from the receipt of the request. Despite the short deadlines it should be noted that when VC are in question, law enforcement, Prosecutors and Courts should act with outmost urgency, due to the high risk of further transferring of VC by the user or a person that has access to the VC in question.[106]

In the ruling of the court for accepting the request of the prosecutor for seizure of the VC, apart from the information included in the request of the prosecutor for seizure, the court must also include the legal grounds for the seizure[107], the value of the VC, the time period for which the VC is seized and the authorities to whom the court decision should be sent.

The value of virtual currencies is not connected to the behavior of a particular economy and depends on the supply and demand of a particular virtual currency. This value is very dynamic and changes on a daily basis. Thus, when stating the value of the VC, the precise day and time when the value was determined should be noted. The value of the virtual currencies is available online for free and the court can consult this value at the time of deciding. Exchangers like Coinbase also provide information about the value of the VC in a given moment.

CPC contains procedural rules regarding the time period for which the seizure can be in force. If the seizure is done in the course of pre-investigative procedure, this measure will end no later than three months from the day that the measure

106 It should be kept in mind that if the user is part of a criminal organization, he/she may not be the only person that has access to the VC. The information for his/her arrest may trigger alarm and the other members of the organized group that also have access to the VC in question may move the VC to other location.

107 The legal bases that enable the court to seize the VC are the ones given article 202 of the CPC

for seizure was enforced, unless investigation is formally opened. In all other cases the seizure can last until the closure of the criminal procedure before the court of first instance. So, the criminal proceedings in which a seizure of VC is being imposed as a temporary measure should be treated by the prosecutors with urgency, since the time frame of three months is not long and cannot be extended. In three months, the prosecutor must provide enough evidence that will either result in an investigation or a closure of the case. Otherwise, despite the fact that the case will not be fully investigated, the prosecutor risks cancelling of the temporary measure and releasing of the VC, so the user will be free to use, manage and transfer them upon own will.

The Court's decision on the seizure of VC needs to be sent without delay to the competent authority for securing the VC.[108] Thus, in its decision the Court must address the question of the competent authority that will enforce the seizure. As a general rule, a competent national authority that is informed without delay for the decision of the court for temporary seizure of property, proceeds or objects is the Agency for managing confiscated assets.[109] If we take a close look at the definitions of the terms "property, proceeds and objects" as given in the Law on managing confiscated property, proceeds and seized objects in criminal and misdemeanor proceedings, it is obvious that these terms follow the meaning defined in the Criminal code. VC fall in this category and as a general rule the Agency for managing confiscated assets is the competent authority for their seizure. However, the law provides a possibility for the Court to decide otherwise and point out the national authority that will be responsible for dealing with the seized property, proceeds or objects. Thus, it is advisable that prosecutors, prior to requesting seizure, know what national authority will enforce the seizure and include that in the request for seizure, together with the public address where the VC should be transferred.

Apart from the general rule that seizure is requested by the public prosecutor, in cases when there is danger of postponement, the members of the judicial police are given the possibility to temporary seize the VC that are instrumentalities of crime.[110] It should be noted that in this case the rules from the CPC that prescribe mandate of the judicial police for seizing VC are lex specialis in comparison with the provisions from the Law on managing confiscated property, proceeds and seized objects in criminal and misdemeanor proceedings, that prescribe mandate of the Agency when it comes to executing the seizure.

This possibility given to the judicial police to act immediately without prosecutor or court prior intervention is of outmost importance when VC are in question,

108 Article 202 paragraph 12 of the CPC

109 Article 24 of Law on managing confiscated property, proceeds and seized objects in criminal and misdemeanor proceedings

110 Article 202 paragraph 6 of the CPC

since it enables timely and prompt reaction of the law enforcement authorities. However, if measures like this are taken by the judicial police, the public prosecutor must be immediately informed and the measures must be than approved by the preliminary judge within 72 hours from the moment of their implementation. If the preliminary procedure judge does not give an approval, the undertaken measures by the judicial police shall be stopped, and any temporarily seized VC shall be immediately returned to the person they were seized from.

In Annex II of the handbook there is a template for motion for issuing temporary safeguarding measures for virtual currencies that are proceeds of crime.

1.1.2. Confiscation of VC as instrumentalities of crime

There are two main types of confiscation of instrumentalities of crime in North Macedonia: 1) mandatory one and 2) discretionary one.

The legal grounds for mandatory confiscation can be found in both the general as well as the special part of the Criminal Code of North Macedonia. Thus, according to the general part of the Criminal code, no one can keep or adopt objects that have occurred through a commission of a crime. Also, objects that were intended or have been used to commit a crime, shall be confiscated from the offender, regardless of whether they belong to the offender or to a third party if this is required by the interest of general safety, health of the people or moral reasons.[111] The special part of the Criminal Code prescribes mandatory confiscation of instrumentalities of crime for specific crimes.

The discretionary confiscation of instrumentalities of crime is regulated in the general part of the Criminal Code where it is stated that objects used or intended to be used to commit a crime may be confiscated if there is a threat that they may be used to commit another crime.[112]

VC can be subject to mandatory as well as under discretionary confiscation, depending on the facts in the case. Confiscation in criminal proceedings, as a general rule is done by the court, with the verdict of conviction. When a mandatory confiscation is prescribed, VC will be confiscated even in the event when the criminal procedure has not ended with a conviction of the defendant.[113]

111 Article 100-a paragraph 1 and 2 of the CC

112 Article 100-a paragraph 3 of the CC

113 Article 529 paragraph 1 of the CPC

Moreover, the decision for seizure shall be enacted by the court, even if the verdict of conviction does not provide for such a decision.[114] This means that in cases of mandatory confiscation of VC as instrumentalities of crime the court acts ex officio. Also, the law provides that when there are factual and legal impediments for conducting a criminal procedure against a perpetrator of a crime, upon a motion by the public prosecutor, the court shall conduct a special procedure for confiscation of instrumentalities of crime, if the conditions provided for in the Criminal Code are met.[115]

Thus, the legal grounds for confiscation of VC as instrumentalities of crime can be found either in article 100-a of the Criminal code, either in specific articles that deal with specific crimes. Also, the legal grounds for mandatory ex-officio confiscation can be found in article 529 of the CPC. In cases where the confiscation is not mandatory and the court does not have a right to act ex officio, it is undisputable that the prosecutor should request confiscation. It should be noted that the terminology used in the law is inconsistent and it creates problems in practice. Thus, the courts in certain occasions use the term "confiscate", whereas in others the term "seizure" and "seize".

When deciding over confiscation of instrumentalities of crime, the court is given the possibility to decide whether the objects that are being confiscated shall be sold according to the provisions valid for enforcement procedure. The proceeds of such a sale shall go to the state Budget of North Macedonia.[116] Thus, if VC are being confiscated, the Court can decide to sell them. The problem here is that the provisions valid for enforcement procedure do not regulate the selling of VC, so it is questionable how the sale will be conducted in practice, in regard of respecting this legal condition for the sale of VC.

The competent authority that should enforce the court's decision for confiscation of the VC according to the Law on managing confiscated property, proceeds and seized objects in criminal and misdemeanor proceedings is the Agency for managing confiscated assets.[117] If the VC are seized prior their confiscation, they will already be on a secure wallet. If VC were not seized prior the final court ruling, their confiscation is questionable since the risks of their disposal are quite high. The current legislation does not provide clear answer on what should the Agency do with the confiscated VC. As it was mentioned, the

114 Article 529 paragraph 3 of the CPC

115 Article 540 paragraph 1 of the CPC

116 Article 135 paragraph 7 and 8 of the CPC

117 Article 28 of the Law on managing confiscated property, proceeds and seized objects in criminal and misdemeanor proceedings states that the decision for seizure of assets, proceeds or instrumentalities of crime is enforced by the Agency. The Agency can ask assistance from the Ministry of interior affairs for the execution of the decision.

Court is the one that decides upon sale of VC, so in cases when there is no court decision for sale of the VC, it is unclear what should the Agency do.

1.2. Seizure and confiscation of virtual currencies as proceeds of crime

In Macedonian legislation the grounds for seizure of proceeds of crime is regulated in the Criminal Code where it is stated that no one may retain the indirect or direct proceeds obtained through a crime, which provides for confiscation of direct[118] and indirect benefit[119], as well as extended confiscation.[120] Apart from confiscation of proceeds of crime from the defendant, the law prescribes possibility to confiscate the proceeds from a third party.[121]

According to the law, subject of confiscation are the money, movables or immovables of certain value, as well as any other ownership, property or active, material or non-material rights, as well as other property corresponding to the value of the obtained benefit in case where confiscation of the obtained benefit is not possible.[122]

Thus, according to these definitions, it is possible to confiscate virtual currencies that are proceeds of crime since they are type of ownership and bring material rights to its owner. Consequently, the VC can be subject of temporary safeguarding measures in the criminal proceedings.

1.2.1. Seizure of virtual currencies as a proceeds of crime

CPC contains procedural rules for issuing temporary safeguarding measures that can help in securing the VC that are proceeds of crime for later confiscation. The temporary safeguarding measures can be issued against the defendant or against third parties who are suspected recipients of assets and property resulting from a criminal offense, without appropriate reimbursement.[123] The temporary safeguarding measures for securing proceeds of crime are the same as the ones that can be issued for securing the instrumentalities of crime.[124]

Thus, the most appropriate temporary safeguarding measure for securing VC as proceeds of crime will be the seizure of the VC. The VC can be seized from the

118 Article 97 of the Criminal code

119 Article 97-a of the Criminal code

120 Article 98-a of the Criminal Code

121 Article 98 paragraph 2 and 3 and article 98-a paragraph 2 and 3 of the Criminal Code

122 Article 98 paragraph 1 of the Criminal Code

123 Article 535 of the CPC

124 Despite the fact that article 535 of the CPC contains technical mistake and revokes to article 194 of the CPC, it is clear that the intention is to revoke to temporary safeguarding measures prescribed in article 202 of the CPC. This kind of approach is being accepted in practice.

defendant as well as from a third party. It should be noted that one VC user can transfer VC from their own wallet, directly to the wallet of another VC user. This transfer can be done without appropriate reimbursement that enables the law enforcement authorities to ask seizure of VC from the third party as well. The appropriate reimbursement for transfer of VC is easy to be determined since the transaction contains data on when the transfer was done and the value of the VC at that precise moment can be consulted online for free. Donation of VC is not unknown, so if a third party receives as a donation VC that are proceeds of crime, this VC can be subject of seizure.

The temporary safeguarding measures are issued by the court upon a request from the public prosecutor. The legal provisions for temporary safeguarding measures for securing instrumentalities of crime apply accordingly in cases of temporary safeguarding measures for securing proceeds of crime. The only difference when requesting temporary safeguarding measures for securing VC as proceeds of crime vs. VC as instrumentalities of crime is the deadlines for the appeal against the court decision.

Consequently, when requesting temporary safeguarding measures for securing VC as proceeds of crime, the public prosecutor should have all the information needed for filing a request for seizure of VC that are instrumentalities of crime. Also, the decision of the court for seizure of the VC as proceeds of crime should contain the same elements as the decision of the court for seizing the VC that appear to be instrumentalities of crime. Thus, the same remarks given in the previous chapter of this Handbook concerning the court decision and the competent authority for execution of the court decision apply.

From a practical point of view, VC can in part be instrumentalities of crime and in part be proceeds of crime. For example VC can be initially bought to cover the illegal origin of the money obtained through drug trafficking. For instance, the suspect owns equipment for mining cryptocurrencies, but in order to avoid paying for electricity used for the mining, he connected to the electricity distribution network directly, so that for a period of one year he was stealing electricity in order to mine cryptocurrencies. Acting in this manner he was able to mine certain number of cryptocurrencies, which from a legal point of view are considered instrumentalities of crime, since they are a product of the suspect's criminal activity. The value of the mined cryptocurrencies increased over time, so the suspect traded the cryptocurrencies on an exchange platform by selling the mined cryptocurrencies and buying new cryptocurrencies. The new cryptocurrencies are in fact the indirect property benefit deriving from the suspect's criminal activity. In cases like this it's irrelevant which legal basis the prosecutor will use for seizure of the VC, since the procedural rules for the seizure are the same and the law provides for possibility a temporary safeguarding measures to be issued for both situations.

The example given In Annex II of the handbook can be used as a template for motion for issuing temporary safeguarding measures for VC that are proceeds of crime as well, by adjusting the legal grounds only.

1.2.2. Confiscation of virtual currencies as proceeds of crime

The confiscation procedure for proceeds of crime is defined in the CPC[125], where it's stated that the assets and the proceeds obtained by committing a crime are determined in the criminal proceedings. The public prosecutor is obliged during the criminal procedure to gather evidence and to examine all circumstances that are important for determining the assets and the proceeds of crime. Thus if VC appear to be proceeds of crime, the public prosecutor should gather evidence that support this and should be able to prove that the VC in question are indeed proceeds of crime, requesting their confiscation.

When VC appear to be proceeds of crime, the user of the VC shall be summoned to be heard during the preliminary procedure and at the main hearing, but the procedure can be conducted in user's absence as well. The user has a right to propose evidence and upon authorization of the Presiding Judge of the Trial Chamber to question the defendant, the witnesses and expert witnesses.

The confiscation of the proceeds of crime is usually imposed by the court in the guilty verdict for the defendant. In the pronouncement of the verdict the court should describe the VC that is being confiscated.

Likewise the confiscation of instrumentalities of crime, the law also stipulates that when there are factual and legal impediments for conducting a criminal procedure against a perpetrator of a crime, upon a motion by the public prosecutor, the court shall conduct a special procedure for confiscation of proceeds of crime, if the conditions provided for in the Criminal Code are met.[126] Thus, for example if the user of the VC dies during the criminal proceeding, the prosecutor can file motion for conducting special confiscation procedure for confiscating VC that appear to be proceeds of crime.

When it comes to execution of the court decision for confiscation of the VC as proceeds of crime, the law stipulated that the court that passed the first instance judgement should issue enforcement order.[127] Having in mind the current legal provisions and the involved law enforcement authorities, in the enforcement order the court should designate the competent authority that will execute the confiscation, that is, as previously explained, the Agency for managing the confiscated assets. In issuing the enforcement order the court should keep in mind

125 Articles 530-541 of the CPC

126 Article 540 paragraph 1 of the CPC

127 Article 541 of the CPC

1) whether the VC were secured with temporary safeguard measure and transferred to a secured wallet and 2) what kind of safeguard measure was imposed. If the VC were secured with temporary safeguard measure and transferred to a secured wallet, the court in the enforcement order can decide upon sale of VC. If the VC were secured and sold, the court can decide the amount received from the sale to be transferred to the Budget of North Macedonia and if the VC were not secured, then it can decide for the VC to be transferred to a secure wallet and sold if this is still possible considering the stage of the proceedings.

1.3. Virtual currencies as evidence in criminal proceedings

VC not only have value, but having in mind the technology they are based on, they can be very useful source of data. The blockchain technology that is used for most of the virtual currencies enables tracking the history of transactions and establishing links between suspects, their co-operators and supporters. Since VC are often used for money laundering purposes, the review of the data sets that the VC hold can point the modus operandi in these cases.[128] Thus VC can also be used as evidence in criminal proceedings as well.

This distinction is relevant from a legal point of view since the CPC of North Macedonia provides different procedural rules for seizing objects that can be used as evidence in criminal proceedings. According to article 194 of the CPC the objects that need to be seized or that can be used as evidence in the criminal proceeding shall be temporary seized and given to the public prosecutor or other authority determined by law or their safeguarding will be otherwise guaranteed. The order for temporary seizure of the objects is issued by the court on the request of the prosecutor or the judicial police. The order for seizure needs to contain: a) the name of the court; b) the legal grounds for temporary seizure, determining the objects that should be seized with precise description; c) name and surname of the person from whom the objects should be seized; d) the place from where the object should be seized; e) the deadline in which the seizure should be done and f) the information regarding the available legal remedies against the court order. In the case of VC, the order for seizure should also include the public address where the VC will be sent and the competent national authority that will enforce the seizure.

128 Europol has supported Spain in dismantling a criminal organisation providing large-scale crypto money laundering services to other criminal organisations. The criminals carried out several money laundering schemes involving the transfer from fiat currency to virtual assets to hide the illegal origin of the proceeds. Some of the identified modi operandi used crypto ATMs and smurfing, a criminal method used to split illicit proceeds into smaller sums and placing these small amounts into the financial system to avoid suspicious transaction reporting. More on: **https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain**

The CPC obliges any person that holds objects that should be seized according to the CC or objects that can be used as evidence to surrender these objects. If the person holding this kind of objects fails to handle the objects to an official person requesting them, a monetary penalty can be imposed to the person.[129] This provision can be used in order to ask a VC user to hand over the private key or the wallet holding VC, since VC can be used as evidence in the criminal proceeding. However, if user of the VC is the suspect, the monetary penalty prescribed in this article cannot be imposed on him.

Another provision that can be useful regarding the detection of VC is the provision under article 181 paragraph 2 and 184 of the CPC, that deal with search of computer system and computer data. The definition of what computer system and computer data are is given in the CC.[130] So apart from body and premises search, the court can issue a search warrant for computer search on basis of elaborated request of the public prosecutor and, if there is a danger of procrastination, upon request by the judicial police.[131] When a search of a computer system and computer data is performed, upon the request of the person that executes the search warrant, the person who uses or has access to the computer or to another device or data carrier shall be obliged to provide access to them and give all necessary information required for unobstructed fulfilment of the goals of the search. Also, there is the obligation on the person using the computer or having access to the computer and other devices or data carriers to immediately undertake necessary measures for preventing the destruction or change of data.[132] Thus, using this provision and having in mind the meaning of the terms, the law enforcement authorities can ask the user or the holder of a cold wallet to give them the password for accessing the wallet.

However it should be emphasized that if a search of computer system and computer data is being conducted, in order to be able to seize the VC, in the request for issuing the search warrant, a request for seizure of VC must be also included, providing information on the public address where VC will be sent, the national authority that will enforce the seizure and the amount of VC that is expected to be seized. If this is not a case and the search warrant does not include request and relevant information for seizing the VC, then a separate court decision for seizing VC must be obtained. As mentioned previously, VC can

129 Article 194 and 195 of the CPC

130 Article 122 paragraph 26 and 27 of the CC. Also, for understanding the scope of the definition for "computer system" the Guidance notes of the Cybercrime Convention Committee (T-CY) on the notion of "computer system" under the Budapest convention can also be consulted **https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090-00016802e79e6**

131 Article 181 of the CPC

132 Article 184 paragraph 1 and 2 of the CPC

be immediately seized by the judicial police as well, but further judicial consent must follow.

In criminal proceedings involving VC it is disputable whether the prosecutors should use the provision from article 198 of the CPC for obtaining relevant data. Namely, article 198 of the CPC deals with temporary seizure of computer data and subject to this provision is any data stored on a computer and similar devices for automatic i.e. electronic data processing, devices used for collection and transfer of data, data carriers and subscriber information at the disposal of the service provider. The prosecutor is entitled to ask this data to be delivered in the deadline he/she has determined. Since in cases of VC, the biggest danger is that the VC will be moved as soon as the user finds out that the law enforcement authorities show interest and this article stands for voluntarily deliverance of the data, it is disputable whether this provision can effectively enable the prosecutor to access the requested data.

However, article 198 can be used to ask the service providers - in cases of VC the exchanges or wallet providers, for data such as subscriber information that they have at disposal. It should be noted that this process is most likely to be followed by MLA request, since most exchanges and wallet providers are located abroad, but the legal grounds for prosecutors to ask such information are found in this article. The prosecutor has authorization to determine the deadline in which the data should be delivered.

In Annex I of the Handbook a template was given on the type of information that can be requested from an exchanger. This template can be used for obtaining information from service providers according to article 198 of the CPC. Here it should be noted that when requesting information from service providers, it is useful to consult the privacy policy and regulations for opening an account with the service providers, since there is information on what are the mandatory information the service providers require form their users, what information they store and for how long.

In Annex II of the handbook a template was given for motion for issuing temporary safeguarding measures for VC and this template can be used to file a motion for seizure of VC in cases when VC were found on grounds of a computer search.

In Annex III of the handbook a template for request for issuing search warrant for computer and computer data search, combined with motion for temporary seizure of the VC is given.

2. INTERNATIONAL LEGAL GROUNDS FOR SEIZURE AND CONFISCATION OF VIRTUAL CURRENCIES OBLIGING NORTH MACEDONIA

There are several international legal instruments that Republic of North Macedonia has ratified, that practitioners should have in mind when dealing with VC in criminal proceedings.

One of the international instruments is the Council of Europe Convention on Cybercrime from 23.11.2001[133], also known as Budapest Convention on Cybercrime that was signed by North Macedonia on 23.11.2001, was ratified on 15.09.2004 and entered into force on 01.01.2005. Republic of North Macedonia does not have any reservations regarding the Convention and only provided information on the competent authority to deal with obligations arising from the Convention as well as 24/7 network point of contact.

The Budapest Conventions prescribes obligation for the states to criminalize offences against computer systems (illegal access, illegal interception, data and systems interference etc.) and offences by means of computers (such as fraud, child pornography and IPR offences)[134], to provide procedural safeguards and tools for securing electronic evidence (search and seizure, expedited preservation etc.)[135] and to engage in efficient international cooperation through a combination of immediate, provisional measures and formal mutual assistance as well as 24/7 points of contact.[136]

From a virtual currencies perspective, in cases when during suspect questioning the suspect admits the use of wallet and provides written consent to the seizure of the VC by means of his computer system, the Budapest convention enables the police to do so immediately in accordance with article 32 b) of the Budapest Convention on Cybercrime without any further procedural requirements.

Other provisions relevant for national authorities when it comes to Budapest Convention are the ones that enable gathering of subscriber information from the service providers. The term “subscriber information” is defined in Article 18.3 of the Budapest Convention where it is stated that for the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

133 **https://rm.coe.int/1680081561**

134 Chapter II, section 1 of the Budapest Convention

135 Chapter II, section 2 of the Budapest Convention

136 Chapter III of the Budapest Convention

a) the type of communication service used, the technical provisions taken thereto and the period of service;
b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Paragraph 177 - Explanatory Report of the Budapest convention[137] furthermore notes that subscriber information refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to address this type of information. "Subscriber" is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

Budapest convention also defines service providers[138], stating that "service provider":

a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
b) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

From a VC perspective, all service providers as wallet providers and exchanges are obliged to provide the subscriber information they have, thus the provisions from the Budapest Convention can be used as legal grounds for requesting the subscriber information.[139]

It should be also noted that Budapest Convention can be used as basis for asking and providing mutual legal assistance in obtaining information and evidence relevant for the criminal investigation involving virtual currencies.[140]

As to the other international instruments that oblige the authorities of North Macedonia, it is worth mentioning that all the international instruments that

137 **https://rm.coe.int/16800cce5b**

138 Article 1.c of the Budapest Convention

139 More details regarding production orders for subscriber information can be found in T-CY Guidance Note #10 **https://rm.coe.int/16806f943e**

140 Chapter III of the Budapest Convention

impose obligation to investigate and prosecute criminal activities that fall in the scope of the conventions and provide for seizure and confiscation of the instrumentalities and proceeds of crime[141], in fact impose obligation in respect to VC as well, since, as explained VC can be instrumentalities and proceeds of crime. Thus, all these international instruments can be also referred as legal grounds for undertaking investigative, preventive and repressive activities in the criminal proceedings in respect to VC.

3. PRACTICAL CHALLENGES FOR SEIZURE AND CONFISCATION OF VIRTUAL CURRENCIES IN CRIMINAL PROCEEDINGS AND OPEN QUESTIONS

Law enforcement authorities in North Macedonia (judicial police and public prosecutors) have legal possibility to request seizure and confiscation of virtual currencies and the courts have legal basis to allow such measures. However, despite the possibility to use the current legal provisions for dealing with virtual currencies in criminal proceedings, the big question on how practically this will be done remains unanswered.

Thus, practitioners are faced with the dilemma a) who will enforce the court decision for seizure or confiscation of virtual currencies and b) how this will be done.

Under the existent legal requirements, the legal entity entitled for enforcing court's decisions for temporary seizure or for confiscation of assets in general including VC, as previously explained, is the Agency for managing confiscated assets. The court can designate another authority if it considers more appropriate, but the general rule is that the Agency for confiscated assets should deal with the seized and confiscated VC. However, when it comes to seizure of VC, power to temporary seize VC is also given to the judicial police.

141 Strasbourg convention - Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (CETS No. 141) **https://www.coe.int/en/web/conventions/full-list?-module=treaty-detail&treatynum=141**; Warsaw convention - Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism **https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=198**; Criminal Law Convention on Corruption (CETS No. 173) - **https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=173**; UN Convention against transnational organized crime - **https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf** etc.

But even if we accept that this dilemma is solved by the legislator, the question how the court decision for seizure or confiscation of virtual currencies will be enforced in practice, remains open.

In order to effectively enforce the court's decision for seizure or confiscation of VC, the VC need to be stored and secured. This is done by transferring the VC from the user's wallet to a secure wallet. The main problem at the moment is that there is no law enforcement authority that owns secure wallet where VC can be transferred, nor opening of such is envisioned. If VC are not transferred to a secure wallet, having in mind that they can be accessed remotely, from different devices, the user is likely to remove them to other wallet or sell them, making all the efforts of the law enforcement authorities in vain.

It should be noted that a seizure of a computer (containing a software wallet), a hardware wallet device and a paper wallet for example is not sufficient. Also, copying a DAT file (containing a wallet) from a computer will not be sufficient. Seizing a computer, or a hardware wallet … is not equal to seizing cryptocurrencies.[142]

Storing and securing VC is not part of any national strategy or other policy document that defines the type of government controlled wallet that should be used as secure wallet or that in any manner address this issue. Thus, law enforcement authorities have a wide range of possibilities when it comes to opening and managing secure wallet.

Apart from storing and securing, VC can also be converted. As previously explained, converting VC means that they should be sold and the money should be deposited on special account. If we analyze the current legal provisions, the Agency for managing confiscated assets may, with the prior consent of the court, make a decision for the sale of the temporarily confiscated movable items if it assesses that the storage of the item reduces its value or the costs for its storage are disproportionately high.[143] Having in mind that according to the Law on ownership and other ownership based rights, movable items are those that can be moved or moved from one place to another, without damaging their essence[144], VC can be considered movable items and thus can be sold even if they are only temporary seized.

However, these provisions do not overcome the difficulties arising from the need to secure the VC. In cases where a decision for selling of VC is being made,

142 "Guide on seizing cryptocurrencies", Cybercrime program office of Council of Europe, February 2021, pg. 24

143 Article 48 of the Law on Law on managing confiscated property, proceeds and seized objects in criminal and misdemeanor proceedings

144 Article 13 of the Law on ownership and other ownership based right (Official Gazette of North Macedonia 18/01, 92/08, 139/09, 35/10)

first VC should be transferred to a secure wallet and then sold. Namely, the Agency can decide to sell the temporary seized VC, but it needs consent of the Court. This means that the Agency should file a motion to the Court requesting consent for selling of the VC in cases the legal conditions are met. It should be noted that these activities happen after the VC have been formally temporarily seized and transferred on a secure wallet.

Despite the fact that there are no specific legal provisions on opening and managing of a secure wallet, each of the law enforcement agencies involved can make decision to open such wallet for the purpose of executing their legal mandate. Namely, according to the Constitution of Republic of North Macedonia, everything that is not prohibited by the Constitution and law is free[145], so law enforcement agencies are free to undertake all necessary measures, which are not prohibited by the Constitution or the law, to secure the full execution of their mandate. Moreover, the international legal instruments that North Macedonia has accepted require from national authorities to undertake all necessary measures that will ensure their full implementation. Thus, each of the law enforcement agencies can opt to open secure wallet and enforce internal procedures/protocols that regulate the opening and managing of the secure wallet. In designing the internal procedures/protocols, special attention should be paid to the question of the type of secure wallet, access to the wallet, the transaction fees and the further managing of VC.

The question that must be addressed by the legislator is what happens with the VC after their final confiscation. According to the existent legislation, the court is the competent authority that decides upon the sale of VC, but this is only a discretionary power of the court and the sale is not mandatory. In cases where there is no court decision for sale of VC, it is unclear what should the Agency do. Thus, it would be of great importance for practitioners if there is a general rule determining the fate of VC after their confiscation. Moreover, the lack of rules can be seen as a possibility for the Agency to keep the VC and decide to sell them later, which might leave space for abuses and can lead to financial losses.

145 Article 8 paragraph 2 of the Constitution of Republic of North Macedonia (Official Gazette of North Macedonia 1/92, 31/98, 91/01, 84/03, 107/05, 3/09, 49/11, 6/19, 39/19)

V. Republic of Slovenia experience in handling virtual currencies in criminal proceedings

Since there are no special provisions that would regulate handling of VC in criminal proceedings in Slovenia, State Prosecutor General of the Republic of Slovenia adopted Decision No. VDT-Tu-15-5/4/2019 appointing a working group responsible for the drafting of guidelines for dealing with criminal offences related to virtual currencies. The working group consisted of a state prosecutor, two legal advisors and two police investigators. The working group has studied the specialised literature available in this field, as well as existing practical examples related to virtual currencies, and has formed a non-binding recommendation for prosecutors. The Guidelines for the investigation of criminal offences related to virtual currencies (hereinafter: the Guidelines) were adopted in November 2019[146]. Relevant sections of the Guidelines are explained below.

1. LEGAL FRAMEWORK

Virtual currency as such is defined by Article 3, point 48 of Prevention of Money Laundering and Terrorist Financing Act (hereinafter ZPPDFT-1B)[147]:

"- virtual currency is 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 exchange and which can be transferred, stored and traded electronically."

This definition of the Directive (EU) 2018/843 (AMLD V) was transposed into Slovenian legal order with the amendment of the ZPPDFT-1B, valid from 11 July 2020.

146 Guidelines for the investigation of criminal offences related to virtual currencies, ref. no. Ktr-zb-9/11/2019/AF-nf, Supreme State Prosecutor's Office of the Republic of Slovenia, November 2019

147 Prevention of Money Laundering and Terrorist Financing Act, Official Gazette of the Republic of Slovenia, no. 68/16, 81/19, 91/20 and 2/21)

Virtual currencies are not considered funds in the Republic of Slovenia. As set out in point five of Article 4 of the Payment Services, Services of Issuing Electronic Money and Payment Systems Act (hereinafter: ZPlaSSIED)[148], funds include banknotes, coins, book money and electronic money. Since the currencies concerned are, as their name would suggest, virtual (more specifically digital records of analogous monetary value), whereas banknotes and coins are issued by the Bank of Slovenia (hereinafter: BS) and the European Central Bank (ECB), virtual currencies cannot be defined accordingly, even though their value can be stored on a medium comparable to a banknote or a coin (e.g., paper [paper wallet] or coin). Similarly, they cannot be defined as book money, i.e., the money entered in the accounts of payment institutions. As set out in paragraph one of Article 24 of the ZPlaSSIED, payment institutions are legal persons established in the Republic of Slovenia that conduct at least part of their payment activities in the Republic of Slovenia and have acquired the appropriate authorisation from the BS; companies that issue, manage or operate virtual currencies, however, usually do not fulfil these conditions. Electronic money refers to stored monetary value in the form of the electronic money holder's claim towards the electronic money issuer, is issued by the electronic money issuer on the basis of receipt of funds for the purpose of making payment transactions and is accepted as a means of payment by a person other than the electronic money issuer (point 11 of Article 4 of the ZPlaSSIED). Virtual currencies therefore cannot be defined as electronic money, since their holders do not have a claim towards their issuers (they have a claim towards unknown users of the virtual currency), and since companies that issue, manage or operate virtual currencies are not the electronic money issuer as defined in Article 158 of the ZPlaSSIED.

Virtual currencies also cannot be defined as foreign cash, as defined in Article 4 of the Foreign Exchange Act (ZDP-2)[149], since they are not banknotes and coins in a foreign currency issued by a central bank or state. Furthermore, virtual currencies are not book-entry securities (Article 4 of the Book-Entry Securities Act – ZNVP-1)[150], since no obligation arises from them, their issuers are not bound by any obligations, and they are not created with entry in the central register of book-entry securities. Lastly, virtual currencies, as defined in point 48 of Article 3 of the ZPPDFT-1, are not financial instruments, as set out in paragraph two of Article 7 of the Market in Financial Instruments Act (ZTFI-1)[151], since they are not transferable securities, money-market instruments or derivative financial instruments.

148 Payment Services, Services for Issuing Electronic Money and Payment Systems Act, Official Gazette of the Republic of Slovenia, no. 7/18, 9/18 and 102/20

149 Foreign Exchange Act, Official Gazette of the Republic of Slovenia, no. 16/08, 85/09 and 109/12)

150 Book-Entry Securities Act, Official Gazette of the Republic of Slovenia, no. 75/15, 74/16 – ORZNVP48, 5/17, 15/18 and 43/19

151 Market in Financial Instruments Act, Official Gazette of the Republic of Slovenia, no. 77/18, 17/19, 66/19 and 123/21

Since the adoption of the euro, the legal tender in the Republic of Slovenia are euro-denominated banknotes and coins (Article 3 of the Euro Introduction Act – hereinafter: ZUE[152]), which does not preclude the use of virtual currencies for business purposes. Since the ZUE does not expressly prohibit such use, persons can agree to use virtual currencies as a means of payment. To wit, performance is the execution of that which is the content of the obligation (paragraph one of Article 282 of the Obligations Code – hereinafter: OZ)[153], whereas an obligation may be such that someone provides something (paragraph one of Article 34 thereof). Since the phrase "provides something" is undefined and can be realised in many different ways, and since a transfer of a virtual currency is not impossible, impermissible, unspecific or unspecifiable (Article 35 of the OZ), the logical conclusion would be that virtual currencies can be used for the fulfilment of contractual obligations if parties have agreed to such use. This conclusion can also be reached on the basis of point 48 of Article 3 of the ZPPDFT-1, which provides that virtual currencies may constitute a direct means of payment between entities that adopt it. Such is also the position of the Court of Justice of the European Union (CJEU) in Case C-264/14 (Skatteverket v David Hedqvist), ruling that Bitcoin is a legal tender, but not tangible property.

In the Guidelines it was suggested that in terms of legal characteristics of a criminal offence, virtual currencies cannot be regarded as movable property or an independent physical object (Article 15 of the Law of Property Code – hereinafter: SPZ[154] and paragraph six of Article 99 of the Criminal Code – hereinafter: KZ-1[155]), since they cannot be made tangible (e.g., put into banknotes or coins with an attributable value), this being the basic precondition for the definition of "a thing".

Nevertheless, the Guidelines stated that virtual currencies merit a sui generis status similar to property rights, since they are transferable, carry an objectively identifiable economic value that can be expressed in terms of money, and can be cashed in or otherwise used for business purposes (Article 22 of the SPZ). In terms of the principle of legal certainty of a criminal law (***lex certa***), the legislator would have to amend the KZ-1 and provide a more specific definition of virtual currencies, modelled on the definitions of energy generated or accumulated for the purposes of lighting, heating, radiation, drive, locomotion or transmission of voice, picture or text across distances (paragraph six of Article 99 of the KZ-1); the legal classification of larceny (Article 204 and other articles thereof) would not be possible.

152 Euro Adoption Act, Official Gazette of the Republic of Slovenia, no. 114/06)

153 Obligations Code, Official Gazette of the Republic of Slovenia, no. 97/07, 64/16 and 20/18 – OROZ631

154 Law of Property Code, Official Gazette of the Republic of Slovenia, no. 87/02, 91/13 and 23/20

155 Criminal Code, Official Gazette of the Republic of Slovenia, no. 50/12, 6/16, 54/15, 38/16, 27/17, 23/20, 91/20 and 95/21

However, after the adoption of the Guidelines, the Supreme Court of the Republic of Slovenia proceeded on a case where the defendant was convicted for the criminal offence of Misappropriation, pursuant to Art. 208 of KZ-1, where the defendant had unlawfully appropriated credit money of an injured party. The Supreme Court of the Republic of Slovenia ruled[156] that the external appearance of money in a tangible or intangible form cannot be decisive for its criminal law protection, since, as is also evident from the titles of Chapter Twenty-three of the Criminal Code, which contain offences of this kind, the protected asset is foreign property, and the principal act of its execution is its deprivation from the possession of the beneficiary or its appropriation. The asset that is affected and protected by criminal law is property in the sense of ownership, as a fundamental right to property, which the perpetrator deprives the beneficiary of, either by appropriating cash or by appropriating credit money, or in both cases by withholding it. It is therefore necessary to agree that it is not in accordance with the law to distinguish between the concepts of ‹tangible› and credit money in the manner used in the judgment under appeal[157], and that such an interpretation would make it impossible to provide effective and comprehensive legal protection against alienation and other related offences. Even though this judgement does not deal with virtual currencies, the interpretation of "tangibility" can be applied also for virtual currencies, suggesting that also criminal offence of larceny would be possible without amending current provisions of KZ-1.

2. INVESTIGATION AND ACQUISITION OF INFORMATION

Considering that virtual currency transactions are normally public and verifiable (exceptions include Monero [XMR], ZCash [ZEC] and some other lesser-known currencies), the investigation of criminal offences can use traditional methods as well as the "follow the money" approach, through the inspection of public ledgers or blocks (e.g. using Chainalysis software). Since users of virtual currencies are anonymous, the purpose of this approach is to

156 Judgement of the Supreme Court of the Republic of Slovenia, ref. no. I Ips 21072/2014 from 15 October 2020

157 Judgement of the Higher Court in Maribor, ref. no. IV Kp 21072/2014 - the judgment was based on the interpretation that attention should be paid to the difference between cases in which money in banknotes and coins can be tangible and, consequently, can be moved without damage to its substance, and cases in which such tangibility is not possible. It pointed out that the essence of things, apart from the fictions referred to in Article 99(6) of the KZ-1, lies in their corporeality, referring to the definition of the concept of thing in Article 15 of the Civil Code, which is not the case with certain types of money (credit money). It explained that, according to the description of the offence, the money in question in the present case was money misappropriated in the form of a remittance, that is to say, credit money as data, and not a thing tangible in the physical form, which that money does not have in appearance

uncover the identity of an unknown perpetrator or to link a known perpetrator to illegal proceeds, which can be achieved by: **a) identifying the provider of the perpetrator›s electronic wallet, b) identifying the IP address of the user of a particular electronic wallet, and c) acquiring the data on the perpetrator›s trading account with the provider of an online exchange.**

The objective of the **first measure (a)** is to acquire as much data created through the use of an electronic wallet for virtual currencies as possible. Some service providers collect a vast array of information on users, such as: personal name, geographical or electronic address, telephone number, scan of a personal ID or a bill proving domicile, transaction account or debit card number, IP addresses and times of access to the wallet, type and version of device, its operating system and web browser (for electronic wallets). If virtual currency transactions are linked to a specific address of a wallet to reveal its provider, some of the information mentioned above can be acquired on the basis of the provisions of Articles 149b and 149č of the Criminal Procedure Act (hereinafter: ZKP[158]). Mentioned articles constitute legal grounds for obtaining data in electronic communication network.[159] Prior to that, the general terms and conditions or the privacy policy of the provider of an electronic wallet (i.e. the information service provider) need to be examined to ascertain if the provider collects personal and traffic data on their users, which data they collect and how long they store it (e.g. by checking their website). Specific measures can be determined (e.g. on the basis of Article 149č of the ZKP for personal name, geographical or electronic address, telephone number, scan of a personal ID or a bill proving domicile, transaction account or debit card number; Article 149b thereof for IP addresses, times of access to the wallet, type and version of device, operating system and web browser) or a preliminary storage of data requested (Article 149e thereof) only after establishing that the service provider collects any of said information, otherwise these measures are not appropriate since their objectives cannot be achieved.

While following the money in the blockchain, a customised software can in some cases directly reveal the IP address of the electronic wallet containing the virtual currency units received **(measure b)**. In this case, the WHOIS software tool can be used to determine the provider or operator managing the IP address, who then transmits the identity of the actual user. If the software tool shows that the IP address is managed by a VPN or VPS service provider, their general terms and conditions or their privacy policy need to be examined (e.g. by checking their website) to ascertain if they collect personal data on their users and how long

158 Criminal Procedure Act, Official Gazette of the Republic of Slovenia, no. 32/12, 47/13, 87/14, 8/16, 64/16, 65/16, 66/17 – ORZKP 153,154, 22/19, 55/20, 89/20, 191/20, 200/20 and 105/21

159 It should be noted that Criminal Procedure Code of Republic of Slovenia does not mention virtual currencies at all, so the existent law provisions are used in cases of virtual currencies.

they store it. In such cases, it is recommended that this data be requested from the information service provider or operator by applying the measures defined in Article 149b of the ZKP, as well as Article 220 thereof in conjunction with Articles 29 and 31 of the Convention on Cybercrime (e.g. for mirror images of rented virtual private servers or mirror images of data media), otherwise (or in cases where IP addresses are routed through Tor, I2P or Freenet networks) this measure is not appropriate since users' identities cannot be efficiently established.

The most optimal means of gathering evidence is proffered by the **third measure (c).** If an inspection of the blockchain indicates that virtual currency units were transferred to an address of an electronic wallet provided by an online exchange, then, by combining the measures defined in Articles 149b (149e in urgent cases) and 156 of the ZKP, the exchange can be requested to transmit all personal, traffic and financial data created by users while disposing of the services of the exchange. We therefore propose that in cases where virtual currency units have been transferred to an address of an electronic wallet provided by an online exchange, the general terms and conditions or the privacy policy of the latter be examined (e.g. by checking the website) and then, depending on the array of data stored, a suitable measure be selected. On the basis of paragraph five of Article 156 of the ZKP, the police will be able to request the personal data (most often personal name, geographical or electronic address, telephone number, scan of a personal ID or a bill proving domicile, transaction account or debit card number) from companies that issue, manage or operate virtual currencies. In other cases, an investigating judge will have to issue a court order for obtaining traffic data (IP addresses, times of access to the wallet, type and version of device, operating system and web browser) pursuant to Article 149b thereof and/or for obtaining financial data pursuant to paragraphs one and three of Article 156 thereof.

3. SECURITY OF CLAIMS AND CONFISCATION OF ASSETS

Since virtual currencies are comparable to property rights, proceeds in the form of virtual currencies can be confiscated from the perpetrators of criminal offences. As provided for in paragraph one of Article 75 of the KZ-1, proceeds gained through or owing to the committing of a criminal offence shall be (among other things, but primarily) confiscated from the perpetrator or recipient of the benefit. This measure is by its nature closer to a civil than to a criminal sanction, since its objective is to achieve restitution, i.e., the restoration of assets and the return to the state prior to the commission of a

criminal offence[160]. This can be achieved on behalf of the injured party also by confiscating virtual currencies from the perpetrator or recipient. In such cases, criminal proceedings may include temporary security of claims for the confiscation of proceeds (Article 109, paragraph one of Article 502 of the ZKP), since virtual currencies allow for it.

As mentioned above, virtual currency units can be considered as the property of an individual, particularly due to their value; specific measures may be imposed based on the provisions of the Claim Enforcement and Security Act (ZIZ). If it is established that the perpetrator or recipient has a trading account opened with a company that issues, manages or operates virtual currencies (i.e., an organisation for payment transactions), the court can order the company to prevent the perpetrator, or any person authorised by the perpetrator from using their virtual currency units.

Said measure is applicable only if funds are deposited in a trading account of an identifiable online exchange or a company that issues, manages or operates virtual currencies. In other cases, where virtual currency units are deposited on perpetrators' or recipients' electronic wallets, and the police have seized electronic devices or physical wallets (Article 220 of the ZKP), it does not necessarily follow that said units have also been seized. In fact, such manner of confiscation represents a security risk, since someone acting on behalf of the perpetrator could access the latter's electronic wallet, seized in its physical form, and irreversibly transfer funds from it. We therefore recommend that the police immediately request permission from known and available users of an electronic wallet or a preliminary written (paragraph two of Article 219a of the ZKP) or urgent oral order (paragraph five of Article 219a thereof) from an investigating judge, since this is the only way to legally access the electronic wallet system. Then, two options are available, the choice of which should depend on which electronic wallet the user has opted for.

Option one

Pursuant to paragraph one of Article 223a of the ZKP, virtual currencies shall be protected by storing them on a different suitable medium, with the medium and the private key enabling its use stored together, while the corresponding file shall be kept in a locked cash register for reasons of security and the prevention of unauthorised access.

Option two

Pursuant to the provisions of Article 502 et seq. of the ZKP, a state prosecutor shall request from an investigating judge, upon the seizure of an electronic

160 Judgement of the Supreme Court of the Republic of Slovenia, ref. no. VSRS I Ips 19290/2017

wallet, an order to a licensed company that issues, manages or operates virtual currencies to transfer virtual currency units, sell them and pay out the equivalent amount in euros to the sub-account for court deposits of the Republic of Slovenia at the Public Payments Administration (hereinafter: UJP) owned by the court that has issued the order. If users do not decide on the method of security, they shall be deemed to accept the risks related to virtual currencies, therefore in such cases one should proceed in accordance with option one.

Virtual currencies are inextricably linked to economic risks as well, since their equivalent amounts in euros or other currencies change rapidly. If the value of secured virtual currency units decreases, a state prosecutor may propose to the court to issue an order for the selling of all virtual currency units (Article 506a of the ZKP) and the transfer of the equivalent amount in euros to the sub-account for court deposits of the Republic of Slovenia at the UJP owned by the court that has issued the order. Prior to such decision, the court must obtain the property owner›s opinion (if the perpetrator or the injured party is known) or serve the summons to issue an opinion (if the perpetrator or the owner of virtual currency units is unknown – paragraph two of Article 506 of the ZKP) on whether the state prosecutor should propose selling the property or not. If the value of a virtual currency increases, a state prosecutor should argue in criminal proceedings that the seized virtual currency units be attributed their gross value. The latter is known in Slovenian case law as "gross principle" meaning that the perpetrators of criminal offences cannot rely on deduction of expenses that are per se illegal, since they are inseparably linked to prior illegal activity or they derive from such activity.[161] Instrument of confiscation of property benefit gained through or owing to the committing of a criminal offence is not dedicated only to restitution, or in other words – to restore financial/asses situation as before the commission of criminal offence but also aiming to prevent possible future illegal activity of the perpetrator.

Since criminal offences and circumstances surrounding them are diverse, investigations may use other approaches and define the acts of perpetrators and other participants differently. Therefore, the present recommendations represent only a working tool to facilitate the investigations of criminal offences involving virtual currencies and should not be regarded as legally binding.

161 See judgement of Supreme Court of the Republic of Slovenia, ref no. I Ips 19290/2017

4. SUBSTANTIVE CRIMINAL PROVISIONS IN SLOVENIAN LEGAL FRAMEWORK[162]

Criminal offences related to virtual currencies can be divided into two main groups (based on cases examined and registered by state prosecutor›s offices): The first group relates to virtual currencies as targets due to their value (e.g. fraud, as defined in Article 211 of the KZ-1), whereas the second group involves virtual currencies as a means for committing other criminal offences (e.g. payment in the context of unlawful trade of illicit substances, as defined in Article 186 thereof).

The first group of criminal offences (virtual currencies as targets due to their value) consists of at least four subgroups, depending on the mode of committing the crime:

a) The first subgroup includes acts in which the perpetrator falsely represents facts and misleads the injured party, so that the latter transfers a number of virtual currency units to the electronic wallet of the former. For instance, perpetrators claim that they raise funds for further investments or that additional funds will be allocated to the users of a virtual currency, and convince the injured party to generate additional (easy) profit and transfer irreversibly a number of virtual currency units to them, but do not fulfil their obligations. In our view, such act by the perpetrator exhibits all signs of fraud as defined in Article 211 of the KZ-1.
b) The second subgroup includes a combination of acts in which perpetrators fraudulently obtain the private key, username or password of the injured party (usually with a phishing e-mail), use this data to access the electronic wallet of the injured party, and seize it or transfer virtual currency units to their own account. Since perpetrators know which data they need in order to acquire the virtual currency units of the injured party, their acts of defrauding the injured party exhibit some characteristics of fraud as defined in Article 211 of the KZ-1. This act, however, is only a preliminary (and essential) stage of a subsequent attack on information systems as defined in Article 221 of the KZ-1. Perpetrators illegally enter an information system, change data (e.g. enter their own information to access and seize the wallet of the injured party), spend funds without authorisation (e.g. for payments)

162 Guidelines for the investigation of criminal offences related to virtual currencies, ref. no. Ktr-zb-9/11/2019/AF-nf, Supreme State Prosecutor's Office of the Republic of Slovenia, November 2019

or transfer them (i.e. reallocate virtual currency units to their own electronic wallets). In such cases, due to the relation of subsidiarity (apparent ideal concurrence) or the exemption from punishment of a preceding act (apparent real concurrence), depending on temporal and spatial correlation between the two acts, perpetrators are only charged with the criminal offence of an attack on information systems as defined in Article 221 of the KZ-1 (or, for the relation of speciality, Article 237 thereof).

c) The third subgroup includes criminal offences in which perpetrators steal a physical wallet containing private keys, use them to access the information system (the electronic wallet of the injured party and consequently the virtual currency system), change data (e.g. enter their own information to access and seize the wallet of the injured party), spend funds without authorisation (e.g. for payments) or transfer them (i.e. reallocate virtual currency units to their own electronic wallets). Such act on behalf of perpetrators exhibits only the signs of an attack on information systems as defined in Article 221 of the KZ-1 (or, for the relation of speciality, Article 237 thereof), since the theft of a physical wallet is already subsumed therein (the relation of subsidiarity – apparent ideal concurrence) or corresponds to a non-punishable preliminary act (apparent real concurrence), depending on temporal and spatial correlation between the two acts. This subgroup covers different modalities of criminal offences, depending on the perpetrator›s intent (for instance, if perpetrators do not know that the wallet contains personal keys and think it is only a regular USB key, which they then overwrite, their act only exhibits the characteristics of larceny, as defined in paragraph two of Article 204 of the KZ-1).

d) Lastly, the fourth subgroup consists of acts in which perpetrators access the information system (the electronic wallet of the injured party and consequently the virtual currency system) unjustifiably (e.g. by hacking), change data (e.g. enter their own information to access and seize the wallet of the injured party), spend funds without authorisation (e.g. for payments) or transfer them (i.e. reallocate virtual currency units to their own electronic wallets), their act only exhibits the characteristics of a serious criminal offence of an attack on information systems as defined in paragraph two of Article 221 of the KZ-1 (or, for the relation of speciality, Article 237 thereof).

The second group relates to criminal offences in which virtual currencies constitute a means of payment or a property acquired in the context of unlawful trade of illicit substances, arms, stolen goods, etc. In this sense, virtual currencies entail only illegal proceeds and do not constitute criminal items protected by these criminal offences.

Since virtual currencies can be attributed a monetary equivalent, it is possible to establish the damage caused or the property benefit gained by the perpetrator through the commission of a criminal offence (paragraph nine of Article 99 of the KZ-1). In our view, due to fluctuations in the value of virtual currencies, the damage or illegal proceeds should be set at the value relevant at the moment when perpetrators have achieved their objective by committing a crime, i.e. obtain virtual currency units. At this moment, perpetrators usually receive virtual currency units as "payment" or prevent the injured party from using such units (e.g. by an irreversible transfer to their own electronic wallet).

Special attention should be given to the criminal offence of money laundering, as defined in Article 245 of the KZ-1. As defined above, the virtual currency systems permit the mixing of virtual currency units so as to increase anonymity. Mixing is most often provided by other users of a specific virtual currency system; for a certain percentage of the transaction, they transfer units of a different virtual currency to a new public address of a particular electronic wallet, thus breaking the chain of transactions made and tracked. This corresponds to layering, i.e. the concealment of the source and ownership of a currency; providers of layering, however, are not criminally liable under Article 245 of the KZ-1. Even if one acted diligently and inspected the blockchain to uncover the source of virtual currency units, one could not and would not know if these units were acquired illegally. The abovementioned, however, does not apply to: 1) the perpetrators of criminal offences who know that their virtual currency units were obtained illegally; 2) the providers of mixing who know or should know (for instance, upon receiving a police notice) that the virtual currency units mixed by them were obtained illegally (paragraph five of Article 245 of the KZ-1).

5. PRACTICAL EXPERIENCE – CASE STUDY

In the following section we will present the first criminal case in Slovenia in which virtual currencies were used for payment of illegal services, provided by the perpetrators. Therefore, obtained virtual currencies constituted crime proceeds that should be seized and confiscated.[163]

In the absence of legal regulation of virtual currencies and hence also the regulation of legally acceptable ways of handling the virtual currencies, prosecutor in charge and the police were faced with important questions related to execution of proper measures that would provide admissible evidence.

163 According to Art. 74 of KZ-1 no one shall retain the property benefits gained through or resulting from a criminal offence. Such property shall be seized based on a court decision establishing the existence of a criminal offence under conditions reffered to in the Criminal Code.

Factual situation

The Specialised State Prosecutor's Office of the Republic of Slovenia (hereinafter: SSPO) received a request for legal assistance from Austrian colleagues asking to start covert parallel investigation against Slovenian nationals on the territory of Slovenia. In Austria criminal proceedings were instituted against their national, accused of buying drugs several times, using specific internet platform that was known worldwide. As a result of his criminal activity, special measures took place in order to identify administrators of internet platform. Austrian authorities were executing different covert and classical investigation measures from May 2014.

Two Slovenian nationals administrated online platform that was set up for selling illicit substances. On the website the customers were provided with the list of substances available and their prices. Although the website was publicly accessible, buyers had to register prior their purchase. The website was running on the server with IP that belonged to a company from Hongkong. Buyers from different countries all over the world were offered various ways of payments; virtual currencies (Bitcoins), transferring money with Western Union and in the beginning also direct payments on company's account in Slovenia – the latter was closed soon and an offshore bank account was established. The shipments came from Slovakia, Czech Republic, Spain and The Netherlands. The website offered no information about the company and its legal representatives. After registration the customers were able to place an order. All further communication was carried out via email.

Special investigative measures

Following special (covert) investigative measures were carried out: secret surveillance, obtaining electronic communication data, interception of communication, undercover operations and obtaining bank information. All evidence, obtained in that way, confirmed the fact that perpetrators had been receiving payments in Bitcoins.

A Specialized Investigation Group was formed in pre-trial procedure. It consisted of SSPO, Office for Money Laundering Prevention and Police investigators. The Office for Money Laundering Prevention requested information from other Financial Intelligence Units across EU and obtained information form FIU Luxembourg, confirming that the accused had bitcoins in their wallets. At the same time FIU Luxembourg sent a report of transactions with Bitcoins that were carried out on trading accounts of the two perpetrators at Bitstamp. All transactions were further analysed by the Office for Money Laundering Prevention. It was confirmed that vast majority of inflows had been done by other persons, identified as buyers of illicit substances and in this context, the funds represented a value gained through commissioning of a criminal offence.

Seizure and confiscation of Bitcoins

Several bitcoin addresses were identified in the course of the investigation, used by two main defendants for receiving payments in Bitcoins. Some of the funds were deposited in a trading account operated by Bitstamp S.A. from Luxembourg. For this one, the court ordered a temporary measure securing a claim for the confiscation of proceeds, following prior reasoned proposal by the state prosecutor. The motion of a prosecutor included detailed reasoning of well-founded suspicion that the perpetrators committed a criminal offence, the existence of illicitly gained value and a risk that the accused person alone or through other persons could use such proceeds for further criminal activities, or could conceal, alienate, destroy or otherwise dispose of it in order to prevent or render its confiscation considerably difficult after the concluded criminal proceedings. The proportionality of the measure was also well explained.

There were also four other addresses identified on basis of the analysis of bank account transactions and during performing special investigative measures (secret surveillance and undercover agent that performed feigned purchases). According to the results of the analysis, one of the perpetrators was regularly cashing in bitcoins at BTC machines in a Slovenian city. That was confirmed with paper receipts recovered during a search of a domicile, secret surveillance and short messages with Bitcoin ATM codes received on the perpetrator's mobile phone. That indicated that not all illicitly gained value received through payment in Bitcoins also remained in Bitcoins.

It was also discovered that all addresses were associated to the same Bitcoin wallet. During first examination of seized electronic devices it was recognized that some of them had BlockChain - Bitcoin wallet app installed. After the new analysis the prosecutor again proposed to the judge (after the indictment was filled) to issue another order for examination — the proposal referred to those bitcoin addresses. Not only to find more Bitcoins or other virtual currencies, the prosecutor expected that with the examination of the newly discovered devices also new solid evidence would be gained, proving those Bitcoins addresses were truly used by defendants in this case in order to receive the payments for their services in Bitcoins. With the same proposal the prosecutor also requested the seizure of electronic data that represented proceeds gained through criminal activity — all Bitcoins. It was very likely that examination of electronic devices and the wallet would reveal there were even more funds stored in the wallet. For the purpose of transferring possibly discovered virtual currencies, a new wallet was set up before the proposal. The address of the wallet was included in proposal and sent to the court. The court followed the proposal and issued an order.

Investigators from Computer Investigation Department examined two iPhones and two iPads that belonged to the two main defendants. They managed to

access the wallet and transfer 34.08752292 Bitcoins to the previously set up wallet.

Open questions

There were numerous questions on how to deal with Bitcoins in this particular case that had to be answered properly in order to ensure:

a) How to properly define VCs in a motion for the court to be able to issue executable order;
b) Obtaining evidence that would be admissible before the court at later stages of criminal proceedings;
c) Seizing, securing and handling virtual currencies in a legally sustainable way.

Seizing the Bitcoins

The first order the court issued was an order addressed to a Bitsamp that had prior blocked the accounts of the accused persons after communication with Slovenian Office for money laundering prevention. They froze all the funds and converted Bitcoins and USD funds into EUR, the sum was transferred to Luxembourg Treasury.

The open question was how to seize and secure virtual currencies related to wallets in exclusive possession of the perpetrators - there is no financial institution or exchange to which an order could be sent in order to be executed. Additional question that arose was how to properly define proceeds that were transformed in virtual currency that has not been defined by Criminal Procedure Law or Criminal Code.

The prosecutor in charge of the case filled a reasoned motion for a search of seized electronic devices for which it was confirmed that it stored a Blockchain – Bitcoin Wallet – an application that enabled access to the wallet of the perpetrators through seized iPads and iPhones. With gained access during the examination of the devices the investigators were aiming to get the evidence on usage of known public addresses for transactions and at the same time to seize and transfer the virtual currencies that represented proceeds gained through criminal activity.

Due to unregulated status of VC, the prosecutor requested the **seizure of electronic data** (Bitcoins). In the same motion the prosecutor proposed to court to order the transfer of virtual currencies that were expected to be found in the wallet. For the reasons of seizure and transfer of found virtual currencies, the Police beforehand set up a new wallet. The prosecutor included the public address for transfer that had been communicated from the Police into the motion. The court followed the proposal and issued an order. During the

examination of electronic devices police specialists for computer examination managed to seize and transfer 34.07755074 Bitcoins to a new wallet.

Ensuring a high level of security

As already explained, seized virtual currencies have to be transferred and properly secured in order to prevent unauthorised access and possible misuse of seized funds. After the execution of order, the paper wallet was created. Public key and private key were printed on a separate sheets of paper. The document containing only public key was transmitted to the court. In order to ensure security and to prevent misuse of the access, the private key was for safety reasons stored in a highly protected environment at the police.

Handling of seized virtual currencies

In this case the defendant requested that seized bitcoins were sold. The judge performed a special hearing where defence lawyer explained the arguments for such request. The main argument was the real fear of loss in value. The defence lawyer stated that at the time of sending the request to the court, the value of Bitcoin was high and that they expected fall in the value of this virtual currency in the near future. The court followed the proposal of the defendant and decided (According to paragraph 2 of 506.a CPA) to sell seized Bitcoins. In the reasoning it stated that due to volatility of this virtual currency long-term forecasts were difficult to predict and that in accordance with the Art. 8 of the Decree on the procedure of handling of seized objects and assets it was necessary to ensure security and profitability, in line with market conditions. It was ordered that the sale would be conducted via Bitstamp, which held the license of Lux Central Bank to perform financial services. The responsibility and the obligation to sell seized Bitcoins was delegated to Commission for seized proceeds. Eventually, seized Bitcoins were sold on Bitstamp Limited exchange and the amount of 210.404,10 EUR was transferred to the court's sub-account. In total, 306.841,09 EUR were confiscated in the end.

Lessons learned

Good international cooperation, swift and coordinated actions of different counterparts and knowledge about the functioning of the system of virtual currencies are crucial for timely seizure, transfer and proper securing of the proceeds gained through criminal activity. Existing legal provisions can be sufficient, if legally admissible interpretation allows that. In Slovenian case there was no need to adapt legal provisions that apply in case of temporary measure securing a claim for the confiscation of proceeds gained through or resulting from a criminal offence.

VI. Conclusions and recommendations

The existent legislation in the Republic of North Macedonia enables seizing and confiscation of virtual currencies. Same as Republic of Slovenia, the existing legal provisions from material and procedural law are defined widely enough allowing for virtual currencies to be seized and confiscated without additional legal provisions to be adopted.

However, when it comes to virtual currencies, the practical enforcement of the general legal provisions in North Macedonia is followed by different challenges and difficulties. Though the current legislation allows law enforcement and judiciary authorities to open secure wallets for the purpose of seizing and freezing VC, there are many open questions like:

- what authority will open the secure wallet;
- what type of secure wallet will be opened;
- how the passwords and access to the secure wallet will be generated and managed;
- when a secure wallet will be opened (for purpose of each investigation, for each VC, for each defendant);
- how the transaction fees will be regulated;
- who will have an access to the wallet and what will be the control mechanisms;
- who will manage the transfer of the virtual currencies to the secure wallet;
- who will manage the virtual currencies after they are transferred onto the secure wallet;
- what will happen after seizure, can virtual currencies be sold, how, when and by whom, etc.

Thus, it is advisable that specific rules regulating seizure and confiscation of VC are adopted. These rules can be either implemented in the procedural law or can be part of a general instruction and bylaws, as the example of Slovenia shows. At the moment, having in mind the existent legislation, adopting internal guidelines and rulebooks will be the most prompt and effective way to address all open questions.

The rules that need to be adopted must address all the above-mentioned questions and other questions that are relevant for successful seizure and confiscation of virtual currencies. Special attention should be paid to the content of the prosecutor's motion and the court order when virtual currencies are in question, due to the specific characteristics of the technological process of seizing VC.

As best practices show, it is advisable that secured wallets are opened on a case-to-case basis. Moreover, secure wallets should be opened separately for each VC and for each defendant, enabling single address for every suspect seizure or confiscation. It is a good practice to prepare the proper seizing address(es) and government-controlled wallet(s) in advance as soon as there is a chance to be confronted with a virtual currency seizure. The secure wallet should be open latest before the prosecutor sends motion to the court for seizing the VC, since the public address should be included in the motion to the court.

Also, if applicable, the creation of the secure wallets and addresses must be done in a safe computer environment and it is strongly recommended having a written step-by-step guide as a projection of the internal rules. Depending on which government-controlled wallet and/or procedure will be used, an option could be to have prepared in advance the seizing address as a QR code to avoid typos. Right before executing a seizure, the seizing address needs to be double-checked to see if the address is correct. A suggestion hereby is to use the four-eye principle in which four eyes can check the correctness of the seizing address and hence safeguard the persons who are seizing the assets.

One very important question that must not be overlooked is the question of what happens with the VC after seizure. Can VC be sold and if so, when and under what conditions? Who will be able to approve the sale and what are the legal aspects that must be taken into account? Since it is clear that this question touches the property rights of the defendants in stages when their guilt is not finally confirmed, it is advisable that specific rules are included in the procedural law. In this light, the possibility for reimbursement to the suspect at a later stage because they are found not guilty needs to be taken into account.

Also, clear rules on what happens with the VC after their final confiscation should be adopted. It is advisable that if they are not yet sold, to do so after the confiscation, since further keeping and dealing with VC can bring financial loss and can undermine all the efforts done in the criminal proceeding. Thus, it is advisable that the law that deals with managing of the confiscated assets includes some very general rules regarding confiscation and sale of VC.

Rules upon the sale of VC in criminal proceedings should also be adopted. The Court, as mentioned, can decide to sell the confiscated VC, but the law on enforcement procedure does not have rules on how to sell VC. Thus it is necessary to include general rules on sale of VC, since their sale is quite different from the sale of other objects and other market rules apply.

To conclude, the topic of VC in the criminal procedures in North Macedonia is quite new. Since most of the concerning legislation is in development phase, this is the perfect timing to join efforts and to address this issue in one comprehensive and uniform way. The practical example and the legal position in

Republic of Slovenia provides know-how for the authorities in North Macedonia on how to address this issue efficiently, making sure it is in line with all EU and international standards.

As Slovenian colleagues experienced, good international cooperation, swift and coordinated actions of different counterparts and knowledge about the functioning of the system of virtual currencies are crucial for timely seizure, transfer and proper securing of the proceeds gained through criminal activity. Thus, apart from improvements in legislation, further efforts on straightening the institutional capacities of the law enforcement agencies and judiciary are essential for efficient seizure and confiscation of VC in criminal proceedings.

BIBLIOGRAPHY

LITERATURE:

1. Basic Manual on Detection and Investigating of the Laundering of Crime Proceeds using Virtual Currencies – UNDOC, June 2014 https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf
2. European Central Bank "Virtual Currency Schemes", October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
3. International Monetary Fund Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf
4. Distributed Ledger Technology (DLT) and Blockchain, FinTech Note no.1, World Bank Group, International Bank for Reconstruction and Development, 2017 - https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf
5. FATF "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf
6. FATF Guidance for risk based approach Virtual Currencies, June 2015 https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
7. FATF Guidance for a risk based approach, Virtual Assets and Virtual Assets Service Providers, June 2019 https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
8. R. HOUBEN and A. SNYERS, "Crypto-assets, Key developments, regulatory concerns and responses", European Parliament Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies study, April 2020, (electronically available via https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf).
9. ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
10. R. HOUBEN and A. SNYERS, "Crypto currencies and blockchain, Legal context

and implications for financial crime, money laundering and tax evasion", European Parliament Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies study, July 2018, (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

11. "Guide on seizing cryptocurrencies", Cybercrime program office of Council of Europe, February 2021
12. The EJCN Virtual Currencies Guide for Judicial Authorities

ELECTRONIC SOURCES:

13. https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp
14. https://www.investopedia.com/terms/b/bitcoin-mining.asp
15. https://cointelegraph.com/bitcoin-for-beginners/how-does-blockchain-work-a-beginners-guide-to-blockchain-technology
16. https://builtin.com/blockchain/blockchain-applications
17. https://www.analyticsinsight.net/real-world-applications-of-blockchain-technologies/
18. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
19. https://en.wikipedia.org/wiki/Unspent_transaction_output
20. https://cryptocurrencyhub.io/exchanger-vs-exchange-which-one-to-choose-73af890dea0a
21. https://cryptocurrencyhub.io/exchanger-vs-exchange-which-one-to-choose-73af890dea0a
22. https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-wallet/
23. https://paxful.com/blog/what-are-public-keys-private-keys-wallet-address/
24. https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-wallet/
25. https://medium.com/hackernoon/crypto-wallet-vs-address-54f7fb980bd3
26. https://thenextweb.com/news/the-differences-between-a-bitcoin-wallet-and-an-address
27. https://en.cryptonomist.ch/2020/08/15/bitcoin-mixers-centralized-decentralized/
28. https://bitcoinmagazine.com/guides/what-are-bitcoin-mixers
29. https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down

30. https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain
31. https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million
32. https://en.cryptonomist.ch/2020/08/15/bitcoin-mixers-centralized-decentralized/
33. https://www.investopedia.com/terms/a/altcoin.asp
34. https://www.binance.com/en/support/law-enforcement

LEGAL SOURCES:

35. 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 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843
36. Cybercrime Convention Committee, T-CY Guidance note #1 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e6
37. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=en
38. Budapest Convention on Cybercrime https://rm.coe.int/1680081561
39. Explanatory Report to the Budapest Convention on Cybercrime https://rm.coe.int/16800cce5b
40. Cybercrime Convention Committee, T-CY Guidance note #10 https://rm.coe.int/16806f943e
41. Strasbourg convention - Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (CETS No. 141) https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=141
42. Warsaw convention - Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&-treatynum=198
43. Criminal Law Convention on Corruption (CETS No. 173) - https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=173

44. UN Convention against transnational organized crime - https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf
45. K45. Criminal Code of North Macedonia, Official Gazette of North Macedonia No 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 and 248/2018
46. Criminal Procedure Code of North Macedonia, Official Gazette of North Macedonia No.150/10, 100/12 and 198/18
47. Law on prevention on money laundering and financing of terrorism, Official Gazette of North Macedonia No. 120/18, 275/19 and 317/20
48. Law on managing confiscated property, proceeds and seized objects in criminal and misdemeanor proceedings, Official Gazette of North Macedonia no. 98/08, 145/10, 104/13, 187/13, 43/14, 160/14, 97/15, 148/15 and 64/18
49. Law on ownership and other ownership based right, Official Gazette of North Macedonia 18/01, 92/08, 139/09, 35/10
50. Constitution of Republic of North Macedonia, Official Gazette of North Macedonia 1/92, 31/98, 91/01, 84/03, 107/05, 3/09, 49/11, 6/19, 39/19
51. Guidelines for the investigation of criminal offences related to virtual currencies, ref. no. Ktr-zb-9/11/2019/AF-nf, Supreme State Prosecutor's Office of the Republic of Slovenia, November 2019
52. Prevention of Money Laundering and Terrorist Financing Act, Official Gazette of the Republic of Slovenia, no. 68/16, 81/19, 91/20 and 2/21
53. Payment Services, Services for Issuing Electronic Money and Payment Systems Act, Official Gazette of the Republic of Slovenia, no. 7/18, 9/18 and 102/20
54. Foreign Exchange Act, Official Gazette of the Republic of Slovenia, no. 16/08, 85/09 and 109/12
55. Book-Entry Securities Act, Official Gazette of the Republic of Slovenia, no. 75/15, 74/16 – ORZNVP48, 5/17, 15/18 and 43/19
56. Market in Financial Instruments Act, Official Gazette of the Republic of Slovenia, no. 77/18, 17/19, 66/19 and 123/21
57. Euro Adoption Act, Official Gazette of the Republic of Slovenia, no. 114/06
58. Obligations Code, Official Gazette of the Republic of Slovenia, no. 97/07, 64/16 and 20/18 – OROZ631
59. Law of Property Code, Official Gazette of the Republic of Slovenia, no. 87/02, 91/13 and 23/20

60. Criminal Code, Official Gazette of the Republic of Slovenia, no. 50/12, 6/16, 54/15, 38/16, 27/17, 23/20, 91/20 and 95/21
61. Criminal Procedure Act, Official Gazette of the Republic of Slovenia, no. 32/12, 47/13, 87/14, 8/16, 64/16, 65/16, 66/17 – ORZKP 153,154, 22/19, 55/20, 89/20, 191/20, 200/20 and 105/21
62. Judgement of the Supreme Court of the Republic of Slovenia, ref. no. VSRS I Ips 19290/2017
63. Judgement of Supreme Court of the Republic of Slovenia, ref no. I Ips 19290/2017

Annex I - Template on the information that can be obtained from an exchanger or other service providers. Note: the data privacy section of each service provider and the section for opening account contain information on data available to the service providers. The example is given for information that can be obtained in general, but in this example, data that Coinbase holds was used.

BASIC PROSECUTOR'S OFFICE

RO/KO no._____

(date, place)

TO

(name of the exchange or service provider)

Subject: Request of service provider data

Before the Basic Prosecutor's Office a criminal procedure is being conducted due to existence of suspicions for crime of _____ according to article _____ of the Criminal Code. One of the aspects of the investigation focuses on data from the virtual currencies trading platform _____ (name of the trading platform like Coinbase).

According to powers authorized to me by article 198 of the Criminal Procedure Code, I hereby requests data regarding the transactions sent from the cluster _____ (specification of cluster of interest):

A. The registration details of the exchanger account(s) that received the virtual currency _____ (name of the virtual currency) into the electronic wallets which are included in the Annex I of this request and which are attached on an optical media:

— the username used;
— the real name used in the KYC client check process - full legal name, date of birth, age, nationality, gender, signature and digital copy of the identity document used to create the accounts (like Passport, Driver's License, National Identity Card, State ID Card, Tax ID number, passport number, driver's license details, national identity card details, visa information or proof of residence);

— the e-mail address used;
— the telephone number;
— home address;
— bank account information;
— payment card primary account number (PAN);
— the date when the account(s) was (were) created;
— the date of the last access of the account(s).

B. Log-in sessions on the respective account(s):
— timestamp logins (timestamp);
— the IP addresses and logging actions on the site during the period [dd/mm/yyy-dd/mm/yyyy];
— browser tracking cookie;
— browser user agent;
— browser http_accept and http_lang;
— geo location/tracking details.

C. Details about the existing VC electronic wallets on the exchanger platform where virtual currency was sent from the cluster _____ (specification of cluster of interest):
— current account(s) balance;
— list of the VC transactions sent from the exchanger account(s) (including internal or external transactions within the platform, towards other wallets or exchangers);
— messages between the user(s) of the exchanger account(s) and other users of this platform.

D. VC trade information (transaction details) relating to the accounts referred to in point C:
— Unique ID - ID number identifying a specific trade;
— Ad Unique - ID number identifying the advertisement which was used to create the trade;
— Online provider - The name of the payment method (Online trades only);
— Buyer - Account username of the exchanger user who is purchasing VC;
— Seller - Account username of the exchanger user who is selling VC;
— Fiat - Trade value denominated in the advertisement;
— VC amount - Trade value denominated in VC;
— Dispute started - Indicates whether or not the trade has been disputed;
— Last message by - shows timestamp of latest user message to trade chat;
— Last admin message - shows timestamp of latest admin message to trade chat;

Additional information that should also be provided is the following:
1. If the accounts referred to in point C were subject to reports regarding the suspected activity;

2. If the named accounts were subject to other requests from the law enforcement authorities.

The answer should be sent to the public prosecutor in a timeframe of no later than 30 days from the receipt of this request.

Public Prosecutor

_____

Annex II - motion for issuing temporary safeguarding measures for VC, that are proceeds of crime and VC, that are instrumentalities of crime

Template 1: Request for issuance of a temporary measure for securing virtual currencies that represent illegal property gain (VC as proceeds of crime)

BASIC PUBLIC PROSECUTOR'S OFFICE

KO / RO no. _____ / _____

(place, date)

TO

BASIC COURT - _____

- Preliminary procedure judge –

_____

In the criminal procedure conducted before this Public Prosecutor's Office under RO/KO no._____, against the suspect _____, due to the existence of grounds for suspicion/reasonable suspicion of having committed a crime _____ under Article _____ of the Criminal Code, based on Article 39 paragraph 2 and Article 353 paragraph 1 related to Article 202 of the Criminal Procedure Law, I submit:

Request for issuance of a temporary security measure - temporary seizure of items (virtual currencies)

From _____'s virtual currency wallet (to give a description of the wallet, for example: where it is located, what type of wallet it is or the wallet identification number, if known) to _____ (name and surname of the person, personal identification number, place of living) to temporarily confiscate items, all _____ (name of the virtual currency, for example bitcoins) located in the virtual currency wallet, which on day_____ in _____ are worth _____ denars.

The temporary seizure of virtual currencies should be carried out by members of the judicial police from _____ (name of the body that will carry out the seizure, e.g., Department of Digital Forensics at the Ministry of Internal Affairs; investigators from the research center, etc.).

The seizure of virtual currencies - _____ (quantity and name of the virtual currency expected to be found in the wallet, for example: 5 bitcoins), to be done by transferring _____ (name of the virtual currency) from the wallet of the security wallet described above with public address number _____ (write only the public address of the security wallet, not the private key!).

After the transfer to _____ (name of the virtual currency), the security wallet is handed over for safekeeping to _____ (the body that will keep the security wallet - the Public Prosecutor's Office, the Ministry of Internal Affairs, the Agency for Management of Confiscated Property, etc.).

Virtual currencies are temporarily confiscated until the end of the procedure before the first instance court.

Explanation

Criminal proceedings against _____ are ongoing before this Public Prosecutor's Office, due to the existence of grounds for suspicion/reasonable suspicion that they have committed a criminal act _____ under Article ___ of the Criminal Code.

Namely, _____ (a brief description of the crime and the circumstances known to the public prosecutor should be given here, along with the evidence on which the suspicion that virtual currencies represent a property gain from the committed crime should be based. In particular, the findings and evidence arising from the fact that the wallet indicated in the application contains virtual currencies and to what extent should be explained.

If there is a great difference between the acquired property gain and the current value of virtual currencies, it is necessary to explain the reasons for such a difference in this section.

In particular, this section should state the findings and, if there is a great difference between the acquired property gain and the current value of the virtual currencies, should explain the reasons for such a difference. It is important to determine the type of virtual currencies that are required to be seized - for example Bitcoin, Ethereum, etc. and their quantity, according to data obtained through the undertaken investigative actions. In this part it is necessary to give a description of the person who owns the virtual currencies and, if it is a third party and not the suspect, it is necessary to explain the legal basis for taking the currencies from the third person - for example when they were transferred to them free of charge).

In this case, and in the case of virtual currencies, there is no doubt that, by the end of the criminal proceedings, it will be particularly difficult or impossible to seize them. Thus, it is not possible to know for sure who has access to the

virtual currency wallet and who can access the wallet remotely and alienate or transfer the virtual currencies to other users. The very circumstances in the case, such as taking steps to protect the anonymity of the person seeking temporary seizure of virtual currencies, suggest that, if these virtual currencies are not temporarily secured, then their seizure by the end of the criminal proceedings will be particularly difficult, i.e. impossible.

For all the above reasons, I request the preliminary procedure judge of the Court to issue a temporary security measure - temporary seizure of items (virtual currencies) _____ (quantity and description of the virtual currency) from the person _____, which are suspected to be illegal property gain.

Public Prosecutor

_____

Form 2: Request for issuance of a temporary measure for securing virtual currencies that, according to the Criminal Code, should be seized (VC as instrumentalities of crime)

BASIC PUBLIC PROSECUTOR'S OFFICE

KO/RO no. _____ / _____

(place, date)

TO

BASIC COURT - _____

- Preliminary procedure judge -

_____

In the criminal procedure conducted before this Public Prosecutor's Office under RO/KO no._____, against the suspect _____, due to the existence of grounds for suspicion/reasonable suspicion of having committed a crime _____ under Article _____ of the Criminal Code, based on Article 39 paragraph 2 and Article 202 of the Criminal Procedure Law, I submit:

Request for issuance of a temporary security measure - temporary seizure of items (virtual currencies)

From _____'s virtual currency wallet (to give a description of the wallet, for example: where it is located, what type of wallet it is or the wallet identification number if known) to _____ (name and surname of the person, personal identification number, place of living) to temporarily confiscate items, all _____ (name of the virtual currency, for example bitcoins) located in the virtual currency wallet, which on day_____ in _____ are worth _____ denars.

The temporary seizure of virtual currencies should be carried out by members of the judicial police from _____ (name of the body that will carry out the seizure, e.g., Department of Digital Forensics at the Ministry of Internal Affairs; investigators from the research center, etc.).

The seizure of virtual currencies - _____ (quantity and name of the virtual currency expected to be found in the wallet, for example: 5 bitcoins), to be done by transferring _____ (name of the virtual currency) from the wallet of the

security wallet described above with public address number _____ (write only the public address of the security wallet, not the private key!).

After the transfer to _____ (name of the virtual currency), the security wallet is handed over for safekeeping to _____ (the body that will keep the security wallet - the Public Prosecutor's Office, the Ministry of Internal Affairs, the Agency for Management of Confiscated Property, etc.).

Virtual currencies are temporarily confiscated until the end of the procedure before the first instance court.

Explanation

Criminal proceedings against _____ are ongoing before this Public Prosecutor's Office, due to the existence of grounds for suspicion/reasonable suspicion that they have committed a criminal act _____ under Article ___ of the Criminal Code.

Namely, _____ (a brief description of the crime and the circumstances known to the public prosecutor should be given here, along with the evidence on which the suspicion that virtual currencies represent a property gain from the committed crime should be based. In particular, the findings and evidence arising from the fact that the wallet indicated in the application contains virtual currencies and to what extent should be explained.

If there is a great difference between the acquired property gain and the current value of virtual currencies, it is necessary to explain the reasons for such a difference in this section.

In particular, this section should state the findings and, if there is a great difference between the acquired property gain and the current value of the virtual currencies, should explain the reasons for such a difference. It is important to determine the type of virtual currencies that are required to be seized - for example Bitcoin, Ethereum, etc. and their quantity, according to data obtained through the undertaken investigative actions. In this part it is necessary to give a description of the person who owns the virtual currencies and if it is a third party and not the suspect, it is necessary to explain the legal basis for taking the currencies from the third person - for example when they were transferred to them free of charge).

In this case, and in the case of virtual currencies, there is no doubt that by the end of the criminal proceedings it will be particularly difficult or impossible to seize them. Thus, it is not possible to know for sure who has access to the virtual currency wallet and who can access the wallet remotely and alienate or transfer the virtual currencies to other users. The very circumstances in the case, such as taking steps to protect the anonymity of the person seeking temporary seizure

of virtual currencies, suggest that if these virtual currencies are not temporarily secured, then their seizure by the end of the criminal proceedings will be particularly difficult, i.e., impossible.

For all the above reasons, I request the preliminary procedure judge of the Court to issue a temporary security measure - temporary seizure of items (virtual currencies) _____ (quantity and description of the virtual currency) from the person _____, which according to the Criminal Code should be seized.

Public Prosecutor

_____

Annex III - templates for request for search warrant in combination with request for temporary seizure of VC

Template 1: Request for issuance of search warrant for a computer system and order for seizure of virtual currencies that represent illegal property gain (VC as proceeds of crime)

BASIC PUBLIC PROSECUTOR'S OFFICE

KO/RO no. _____ / _____

(place, date)

TO

BASIC COURT - _____

- Preliminary procedure judge -

_____

In the criminal procedure conducted before this Public Prosecutor's Office under RO/KO no._____, against the suspect _____, due to the existence of grounds for suspicion/reasonable suspicion of having committed a crime _____ under Article _____ of the Criminal Code, based on Article 39 paragraph 2 and Article 181 paragraph 2 related to Article 184 and 186, as well as Article 194 of the Criminal Procedure Law, I submit::

1. **Request for issuance of search warrant for computer systems** – electronic devices owned and used by _____, as follows:

   a. Tablet _____, model _____, with serial number _____

   b. Mobile phone brand _____, model _____, IMEI number _____, with SIM card from the operator _____ with telephone number _____ and serial number _____

   c. Laptop brand _____, model _____, with serial number _____

- me qëllim të gjetjes së sendeve të rëndësishme për procedurën penale, në pajtim me nenin 182 paragrafi 1 të LPK-së.

2. **Request for issuance of an order for temporary seizure of items (electronic data) that can serve as evidence in the criminal proceeding and that represent illegal property gain** and all of them are _____

(name of the virtual currency, for example bitcoins) located in the virtual currency wallet available on the electronic devices described in item 1.

The search of the computer systems and the seizure of electronic data should be carried out by members of the judicial police from _____ (name of the body that will carry out the seizure, e.g. Department of Digital Forensics at the Ministry of Internal Affairs; investigators from the Skopje research center, etc.) whose orders are forwarded together with the seized electronic devices, and the members of the judicial police are to deliver the order directly to the parties.

The search should be conducted by members of the judicial police with access to the virtual currency wallet installed on the electronic devices described in item 1.

The objects, i.e., the electronic data need to be seized without delay by the owner and the user of the electronic devices described in item 1 - _____ (name and surname of the person).

The seizure of electronic data - _____ (quantity and name of the virtual currency expected to be found in the wallet, for example: at least 5 bitcoins), to be done by transferring _____ (name of the virtual currency) from the wallet in which they are found to the security wallet with address number _____ (write only the public address of the security wallet, and not the private key!).

After the transfer of _____ (the name of the virtual currency), the security wallet is handed over for safekeeping to _____ (the body that will keep the security wallet - the Public Prosecutor's Office, the Ministry of Internal Affairs, the Agency for Management of Confiscated Property, etc.).

Explanation

Criminal procedures against _____ are ongoing before this Public Prosecutor's Office, due to the existence of grounds for suspicion/reasonable suspicion that they have committed a criminal act _____ under Article ___ of the CC.

Namely, _____ (a brief description of the crime and the circumstances known to the public prosecutor should be given here, along with the evidence on which the suspicion that the virtual currencies represent a property gain from the committed crime should be based. In particular, the information regarding the existence of a virtual currency wallet on the devices and from where the suspicions arise that it contains virtual currencies and to what extent should be explained. It is important to determine the type of virtual currencies that are required to be seized - for example Bitcoin, Ethereum, etc. and their quantity, according to the data obtained through the undertaken investigative actions.)

Given all of the above, it is likely that _____ (name of the virtual currency, e.g., bitcoin) wallet, and _____ (name of the virtual currency, e.g., bitcoin) will be found in the computer systems - electronic devices owned by _____. These are important items in the criminal procedure because they are suspected to be illegal property gain from the committed crime, as explained above. From the findings of the investigation so far, there are at least _____ (name of the virtual currency, e.g., bitcoin). The probability that these items relevant to the criminal procedure will be found in the computer systems of _____ (name and surname of the person) arises from _____ (to state the information that the public prosecutor has).

For all of the above reasons, I request the preliminary procedure judge of the Court to issue a search warrant for a computer system - electronic devices owned and used by _____, for the purpose of locating and seizing items relevant to the criminal procedure, as well as an order for temporary seizure of items (electronic data) which can serve as evidence in the criminal procedure and which are suspected to be illegal property gain.

Public Prosecutor

_____

Template 2: Request for issuance of search warrant for a computer system and order for seizure of virtual currencies that according to the Criminal Codeshould be seized (VC as instrumentalities of crime)

BASIC PUBLIC PROSECUTOR'S OFFICE

KO/RO no. _____ / _____

(place, date)

TO

BASIC COURT - _____

- Preliminary procedure judge –

_____

In the criminal procedure conducted before this Public Prosecutor's Office under RO / KO no._____, against the suspect _____, due to the existence of grounds for suspicion / reasonable suspicion of having committed a crime _____ under Article _____ of the Criminal Code, based on Article 39 paragraph 2 and Article 181 paragraph 2 related to Article 184 and 186, as well as Article 194 of the Criminal Procedure Law, I submit:

3. **Request for issuance of search warrant for computer systems** – electronic devices owned and used by _____, as follows:

   a. Tablet _____, model _____, with serial number _____

   b. Mobile phone brand _____, model _____, IMEI number _____, with SIM card from the operator _____ with telephone number _____ and serial number _____

   c. Laptop brand _____, model _____, with serial number _____

- for the purpose of finding objects important for the criminal procedure, in accordance with Article 182 paragraph 1 of the Criminal Procedure Law.

4. **Request for issuance of an order for temporary seizure of items (electronic data) that according to the Criminal Law should be seized** and all of them are _____ (name of the virtual currency, for example bitcoins) located in the virtual currency wallet available on the electronic devices described in item 1.

The search of the computer systems and the seizure of electronic data should be carried out by members of the judicial police from _____ (name of the body that will carry out the seizure, e.g., Department of Digital Forensics at the Ministry of Internal Affairs; investigators from the Skopje research center, etc.) whose orders are forwarded together with the seized electronic devices, and the members of the judicial police are to deliver the order directly to the parties.

The search should be conducted by members of the judicial police with access to the virtual currency wallet installed on the electronic devices described in item 1.

The objects, i.e., the electronic data need to be seized without delay by the owner and the user of the electronic devices described in item 1 - _____ (name and surname of the person).

The seizure of electronic data - _____ (quantity and name of the virtual currency expected to be found in the wallet, for example: at least 5 bitcoins), to be done by transferring _____ (name of the virtual currency) from the wallet in which they are found to the security wallet with address number _____ (write only the public address of the security wallet, and not the private key!).

After the transfer of _____ (the name of the virtual currency), the security wallet is handed over for safekeeping to _____ (the body that will keep the security wallet - the Public Prosecutor's Office, the Ministry of Internal Affairs, the Agency for Management of Confiscated Property, etc.).

Explanation

Criminal procedure against _____ are ongoing before this Public Prosecutor's Office, due to the existence of grounds for suspicion / reasonable suspicion that they have committed a criminal act _____ under Article ___ of the Criminal Code.

Namely, _____ (a brief description of the crime and the circumstances known to the public prosecutor should be given here, along with the evidence on which the suspicion that the virtual currencies represent items that according to Criminal Codeshould be seized. In particular, it is necessary to give information regarding the existence of a virtual currency wallet on the devices and the source of the suspicions that it contains virtual currencies and to what extent. It is important to determine the type of virtual currencies that are required to be seized - for example Bitcoin, Ethereum, etc. and their quantity, according to the data obtained through the undertaken investigative actions.)

Given all of the above, it is likely that _____ (name of the virtual currency, e.g. bitcoin) wallet, and _____ (name of the virtual currency, e.g., bitcoin) will be found in the computer systems - electronic devices owned by _____. These

are important items in the criminal procedure because they represent items that according to Criminal Codeshould be seized, as explained above. From the findings of the investigation so far, there are at least _____ (name of the virtual currency, e.g., bitcoin). The probability that these items relevant to the criminal procedure will be found in the computer systems of _____ (name and surname of the person) arises from _____ (to state the information that the public prosecutor has).

For all of the above reasons, I request the preliminary procedure judge of the Court to issue a search warrant for a computer system - electronic devices owned and used by _____, for the purpose of locating and seizing items relevant to the criminal procedure, as well as an order for temporary seizure of items (electronic data) that should be seized according to Criminal Code.

Public Prosecutor

_____

Follow OSCE

OSCE Mission to Skopje
Bulevar 8-mi Septemvri No. 16, 1000 Skopje
e-mail: info-MK@osce.org
website: http://www.osce.org/mission-to-skopje