8th International Scientific Conference ITEMA 2024 – Conference Proceedings
DOI: https://doi.org/10.31410/ITEMA.2024.229

Cryptocurrencies and the Legislative Provisions for the Prevention of Money Laundering in the Republic of Slovenia

Franc Pozderec[1]
Ivanka Oberman[2]

Received: January 3, 2025
Accepted: January 31, 2025
Published: June 2, 2025

Keywords:
Cryptocurrencies;
Legislative provisions;
Money laundering

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission.

Abstract: *Cryptocurrencies represent the future of the digital money system. It is an innovative online payment system that allows transactions to be recorded using decentralised accounting without the control of a central institution. There´s a high degree of user anonymity and users can further obscure the transaction trail by using various anonymisers. Cryptocurrencies are based on a complex infrastructure involving a large number of so-called miners and users coming from different countries, and transactions are validated and recorded globally, making it impossible for Anti-Money Laundering authorities to obtain relevant information on suspicious transactions.*

The present article deals with cryptocurrencies and the process of »mining«, which is the process of validating transactions on a cryptocurrency network and adding them to a blockchain. Also, money laundering issues are highlighted and the Slovenian legislative provisions in this area are presented. Finally, guidelines to prevent money laundering are presented.

1. DEFINITION OF CRYPTOCURRENCIES AND RELATED TERMS

The rise of internet technology and innovation in finance has introduced a completely new currency that is exclusively electronic and brings with it a wealth of new financial possibilities. Digital money relies on information systems and solutions that allow the rapid exchange of data between two entities. In line with this, the concept of decentralisation has emerged, which is completely opposed to the centrally coordinated monetary system that was in place before the rapid rise of digitalisation (Glaser et al., 2014). Cryptocurrency can be defined as any form of currency that exists digitally or virtually and uses cryptography to secure transactions. Cryptocurrencies do not have a central issuing or regulatory authority but use a decentralised system to record transactions and issue new units. They operate on a distributed public ledger called a »blockchain«, which is a decentralized ledger of all transactions, and is updated and maintained by the holders of the currencies. It is therefore a digital payment system that does not use a bank to verify transactions and therefore there is no money in physical form. Cryptocurrency payments exist only as digital entries in an online database where certain transactions are recorded (Ashford, 2023). Nowadays, cryptocurrencies can be purchased through central exchanges, brokers and individual currency owners. The simplest way to buy and sell cryptocurrencies is through exchanges or online platforms such as Coinbase[3]. Crypto wallets exist in two forms: software and hardware. Software wallets can be downloaded onto a computer or phone, while hardware wallets are physical vaults that store cryptocurrency data on a specially designed hard drive in the device. Hardware wallets are designed to be as secure as possible and can be backed up in multiple ways (Suratkar et al., 2020).

[1] New University, European Faculty of Law, Delpinova Street 18/b, 6000 Nova Gorica, Republic of Slovenia
[2] New University, European Faculty of Law, Delpinova Street 18/b, 6000 Nova Gorica, Republic of Slovenia

[3] Coinbase is a cryptocurrency exchange where popular coins such as Bitcoin, Ethereum and Solana can be purchased. While there are thousands of different cryptocurrencies available worldwide, the Coinbase platform hosts more than 260 different types of cryptocurrencies, allowing trading in the most popular types of cryptocurrencies (Haegele, 2024).

OPEN ACCESS

1.1. Decentralisation

Decentralisation means dispersing the departments of a large organisation away from a single administrative centre. In the case of Bitcoin, this can be explained by the fact that Bitcoin is the first cryptocurrency and decentralisation means that no single entity can gain control of the network. The network is based on two pillars, i.e. individual Bitcoin nodes (so-called »full nodes«) and the computing power of the miner. In principle, a node can be operated by anyone by installing the Bitcoin Core Wallet and downloading the Blockchain in its entirety (all transaction data since bitcoin has existed). It then lets the wallet calculator run on the computer, thus contributing to the decentralisation of bitcoin. Many individual network nodes ensure that the Blockchain technology itself is stored in many different locations and that new transactions can be distributed. The basic principle of decentralisation is that no one gets full control over the operation of the Bitcoin infrastructure (Vidrih, 2019).

2. BLOCKCHAIN

Blockchain[4] (blockchain technology) is a type of distributed ledger technology that stores and transmits information in the form of blocks of data linked by a chain of data. The data in a blockchain is cryptographically protected and the mechanism uses specific mathematical algorithms to verify and create a constantly growing chain of databases (the chain of transactions can only be extended and existing data cannot be removed) that form transaction blocks. The system allows for a relatively secure and pseudonymous transfer of value directly between individual entities (peer to peer transactions), independent of the trust and existence of a central entity, as it is collectively maintained and controlled by a distributed network of participants (computing nodes) (Bank for International Settlements, 2018).

When a miner creates a new block of transaction data, information about it starts to be shared across the network in an encrypted form that makes the details of the transactions unavailable to the public. All miners then jointly decide on the validity of the new block of information (consensus mechanism), based on a predefined algorithmic method. The network always considers the longest blockchain as valid. Once validated, the new block is integrated into the blockchain, as evidenced by the update of all copies of the distributed record in the network at the same time. Thus, each miner has an identical copy of the entire transaction record at all times, which is encrypted in such a way as to prevent reversibility of transactions (World Bank Group, 2017).

3. TYPES OF CRYPTOCURRENCIES

Cryptocurrencies can be divided into cryptocoins and crypto tokens, depending on how they are used. Some are intended as units of exchange for goods and services, others are stores of value, and some can be used to participate in specific software applications such as games and financial products (Rosen, 2024).

3.1. Bitcoin

Bitcoin is the most popular cryptocurrency. In January 2009, a mysterious pseudonymous man named Satoshi Nakamoto introduced Bitcoin, which offered lower transaction fees than other

[4] Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets across a business network. Almost anything of value can be tracked and traded on a Blockchain network, reducing risk and costs for all involved (IBM., n.d.).

traditional payment mechanisms. Bitcoins are held only in digital form, where they are kept as balances in a public ledger that everyone has access to. Miners are responsible for processing transactions on the blockchain and are rewarded for their work with fees paid in bitcoins. In 2010, Bitcoin started to appear on exchanges, making it easier to sell, buy, trade and store. In the following year, miners and programmers started to build other networks, such as Etherium and Litecoin. The use of Bitcoin as a currency increased as selected companies started to accept Bitcoin as a means of payment alongside traditional currencies. In total, only 21 million bitcoins can be minted. In April 2022, slightly more than 19 million total bitcoins had been minted (Likos & Hicks, 2022).

3.2. Etherum

Ethereum is the second-largest cryptocurrency by market value as of January 2022. It is essentially a platform based on blockchain technology. It maintains a vast network of computers around the world and requires majority agreement for any change to the blockchain. The Ethereum platform is designed to support multiple applications, not just Ethereum and other cryptocurrencies. It differs from Bitcoin in that, among other things, the Bitcoin blockchain was created with the sole purpose of supporting the Bitcoin cryptocurrency, whereas Ethereum is a network with a lot of programming possibilities for many applications. The number of Bitcoins that can enter circulation is limited to 21 million, while the amount of Ethereum that can be generated is unlimited (Frankenfield, 2022).

3.3. Tokens

Tokens are a programmed digital asset that operates on an existing blockchain. They can represent specific units of an existing asset, such as money or electricity, and are also used to create and enforce unique smart contracts that are executed when certain conditions are met. Tokens can be classified into the following categories (Copeland, 2023):

- Utility tokens are used as a means of transaction or investment and also play a role within a blockchain. For example, a cloud storage project using a blockchain may allow the purchase of a larger memory capacity using tokens of use value.
- Security tokens are used to buy, sell and track ownership of projects or companies. Unlike other tokens, security tokens are the only ones that have laws and rules of use in order to protect investors.
- Stablecoin was created to counter the large fluctuations in the value of cryptocurrencies. They do this by being tied to stable assets such as commodities or cash.
- Privacy tokens were created to ensure anonymity. Examples of such cryptocurrencies are Monero and Zcash. Monero uses a special technology called »ring signatures« to obscure the details of a transaction, while Zcash uses a special technology called »Zk-SNARK« that allows the verification of a single transaction without revealing its details.
- Non-fungible tokens (NFTs) are a unique form of digital asset and have their own value. NFT tokens are therefore primarily used for the ownership of digital art, which takes the form of music, digital artwork, virtual real estate and virtual worlds.

4. MINING CRYPTOCURRENCIES

It is the process of verifying transactions on a cryptocurrency network and adding them to a blockchain. By doing this, miners help protect the network and are rewarded with small amounts of cryptocurrency. Bitcoin uses a proof-of-work (PoW) consensus algorithm that requires miners to perform complex mathematical calculations in order to add new blocks to the blockchain. Each

time a miner successfully compacts a block, he is rewarded with a certain amount of bitcoins. Miners use specialised computers to perform the necessary calculations. These devices are usually equipped with high-performance graphics processing units or specific integrated circuits designed specifically for cryptocurrency mining. Miners need to continuously upgrade their hardware to remain competitive (Fortuna, 2022).

5. CRYPTOCURRENCY TRANSACTIONS

The main purpose of cryptocurrency trading is to make a profit. The advantages of buying and selling cryptocurrencies are the all-day open market, the anonymity of transactions, the immediacy of the transaction and the drastic fluctuations that offer traders the possibility of making a quick profit (Fang et al., 2022). A cryptocurrency transaction is a multi-step process that allows Bitcoin to be transferred from one user to another. The transaction from start to finish is illustrated in the following steps (Viitaharju, 2024):

1) The transaction phase is where the essential information for the transaction is determined and the user selects three options, namely the sending address, the receiving address and the amount to be sent, and then completes the transaction by pressing the 'Send' or 'Withdraw' button, including a digital signature.
2) In the broadcast phase, the details of the transaction are sent to the Bitcoin network, where servers, known as nodes, that store the history of the Bitcoin network ensure that the transaction complies with the rules of the Bitcoin network. Once the nodes have verified that the transaction is correct, the transaction moves to a holding area called the Mempool (short for memory area).
3) The last stage of a Bitcoin transaction is the settlement of the transaction. Miners compete with computing power to see who can solve the problem first and add the next block to the Bitcoin blockchain. Once confirmed, the new block is added to the blockchain copy of all participants on the network. At this point, the transaction and the new block are considered as confirmed. Over time, a practice has been established that prevents a transaction from being duplicated or cancelled after the creation of a new block, which may occur due to a temporary deadlock in the blockchain.

6. ONLINE SCAMS AND FRAUD

There are a variety of scams in the crypto world, such as the following (Republic of Slovenia, Ministry of the Interior, 2022):

6.1. Email intrusions or so-called BEC fraud

In Buisness Email Compromise (BEC) fraud, the perpetrators hack into the email server and use special filters to search for messages that contain information about the transaction that is currently being concluded. The perpetrators set up the forwarding of the received messages to their e-mail address and informed the other business entity that they had changed the account number. Once the transaction has been made to the perpetrator's account, the perpetrator then transfers the funds to a third-country account or makes a cash withdrawal (Republic of Slovenia, Ministry of Internal Affairs, 2018).

6.2. Investment fraud

Such schemes are advertised through social networking profiles and phone calls to random numbers. The fraudster poses as a crypto exchange employee and falsely represent to the victim that there

are funds of several thousand euros waiting for them in a virtual wallet. The withdrawal of these funds is conditional on the installation of a remote access programme (Anydesk, Supremo, etc.) on the computer and/or mobile device. With the help of this application, the perpetrators enter the victim's online bank and steal all the funds from the transaction account (Republic of Slovenia, Ministrstvo za notranje zadeve, 2024).

6.3. Phishing

This type of online fraud usually starts with a fake email or SMS message on behalf of the bank where the perpetrators falsely state various needs for action by the online bank user (e.g. an urgent update or upgrade of e-banking). The message usually contains a link that needs to be clicked. When the link is clicked, a web page identical to the e-banking website is opened. In some cases, once the victim has entered the required information, fraudsters obtain all the necessary information for unauthorised access to the online bank and subsequently empty the victim's bank account (Republic of Slovenia, Ministrstvo za notranje zadeve, 2024). Data fishing via private messages or so-called Smishing works on the same principle, except that the victim receives a message with a link to a fake site via SMS, or an app such as Messenger, Viber, Whatsapp, etc. In most cases, these attacks aim to obtain the username and password of the victim's social network (Safe on the Internet, 2024). Anyone can request a phishing website of their preferred post office or bank from different providers, and payment for subscribing to such a service is most often made in cryptocurrencies (Becher, 2024).

7. LEGAL FRAMEWORK FOR CRYPTOCURRENCY OFFENCES

The fundamental duty of the police is to ensure the safety of individuals and communities, respect human rights and fundamental freedoms, and strengthen the rule of law (Žaberl et al., 2017).

Criminal offences in the Slovenian legal order are defined by the Criminal Code (KZ-1), which, in accordance with the principle of legality, defines them clearly, precisely and in advance at the statutory level (Criminal Code, 2012). The Criminal Procedure Act is essentially a procedural law, the purpose of which is to ensure the effective investigation of criminal offences, while regulating the repressive powers of state authorities and ensuring fair procedure and trial for those involved in criminal proceedings (Šepec, 2023). While the Criminal Code penalizes offenses and defines their sanctions, the Criminal Procedure Act lays down procedural rules for implementing the provisions of substantive criminal law, thereby primarily ensuring that someone innocent is not convicted (Constitution of the Republic of Slovenia, 1991).

7.1. The offence of Money Laundering

Money Laundering is the process of concealing the link between an illicit source of profit and the underlying criminal activity (International Monetary Fund, 2014). The offence of Money Laundering is defined in Article 245 of the Criminal Code (KZ-1), which reads: 'Whoever, by laundering or attempting to launder, conceals the origin of money or property which he has received, kept, used in an economic activity or in any other way, and who knows or ought to have known that it has been obtained by means of a criminal offence, has committed a criminal offence' (Criminal Code, 2012).

According to Article 2 of the Law on Prevention of Money Laundering and Terrorist Financing (ZPPDFT-1), Money Laundering is defined as »any conduct which conceals the origin of money

or other property obtained through a criminal offence, and includes: exchange or transfer in any way money or other property derived from the offence (ZPPDFT-1, 2016).

There are three phases of money laundering (Lamberger, 2009):

1) **Money transfer/placement:** this step represents the starting point of money laundering, which is characterised by the conversion of the form of the primary asset. The process takes place by the offender handing over or electronically transferring money to the launderer. The launderer is a person who is not connected to the offence or any other offence. The reason for this is that he/she has no problem opening a new bank account or smuggling money across the border, where he/she exchanges the money at a money changer or deposits it in a bank account.
2) **Layering:** the second stage of money laundering occurs when dirty money enters the financial system. In order to hide the origin of the money, launderers make a large number of random international transactions to different banks around the world, making it difficult to trace. A certain degree of anonymity allows for the fact that, in the course of business, the details of the directors and beneficial owners are concealed and are not written on any public document or register. Another characteristic of offshore companies is that in most cases financial and legal information is not passed on to foreign tax and judicial authorities.
3) **Integration:** this stage occurs when the money trail has been successfully covered and several layers have been stacked between the source and the laundered money. In this phase, the money is integrated into the legitimate financial system, allowing the money to be disposed of as if it had been legitimately obtained in the first place. The money obtained is then often invested in legitimate activities and some cases reinvested in criminal activity.

7.2. Money laundering through cryptocurrencies

Like accounts in the traditional banking system, bank wallets are susceptible to restrictions on record-keeping and identification of account holders. In a digital environment, it is difficult to track blockchain transactions through IP address anonymisers[5] . IP anonymisers mask the actual location of the wallet owner and mixers help to conceal the origin of funds. Cryptocurrencies pose a risk of money laundering due to the lack of regulation and specific features such as: the decentralisation of the system, the pseudonymity of users and the international nature of the system. The Bitcoin protocol does not require any identification of users in order to use the system and is not verified, nor is any identification data recorded in the transaction log, but transactions are only recorded using users' public keys. The absence of a central institution overseeing the cryptocurrency system prevents AML authorities from obtaining relevant data on suspicious transactions and customers across the cryptocurrency system. As a result, AML regulation is focused on specific intermediaries in the system where cryptocurrency transactions are at least partially centralised (FATF Report, 2014).

8. PREVENTION OF MONEY LAUNDERING IN THE REPUBLIC OF SLOVENIA

As a member of the European Union, Slovenia's laws and regulations on Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) are aligned with EU legislation. The following EU directives are particularly relevant in this field (OpenAI, 2024):

[5] An IP address anonymiser is a tool or technology that allows you to hide or disguise the actual IP address of a user in order to protect their privacy and reduce the tracking of their online activities. The main goal of an IP address anonymiser is to prevent third parties, such as ISPs, advertisers, or even webmasters, from collecting information about a user's network behaviour, such as websites visited, location, device, etc. (OpenAI, 2024).

1) Directive (EU) 2015/849 on the prevention of money laundering (4th Money Laundering Directive): is the key piece of legislation setting out the basic measures to prevent money laundering and terrorist financing in the EU. It includes the following important provisions:
   - Know Your Customer (KYC) obligations: under this Directive, financial services firms (including those dealing in cryptocurrencies) are obliged to verify the identity of their customers and monitor transactions for possible suspicious activity.
   - Extension of scope: the Directive extends the scope to »third country residents« and includes new obligations for companies offering cryptocurrency services (e.g. crypto exchanges and cryptocurrency exchange platforms).
   - Suspicious transaction reporting obligation: financial institutions, including cryptocurrency exchanges, are obliged to report suspicious transactions.
2) Directive (EU) 2018/843 amending and supplementing the 4th Directive (5th Money Laundering Directive): the provisions of that Directive include significant changes that have had a direct impact on the treatment of cryptocurrencies:
   - Explicit inclusion of cryptocurrencies: the cryptocurrency providers (e.g. crypto exchanges, brokers and exchange platforms) must also comply with the same legal requirements as traditional financial institutions, including obligations to verify customers and monitor suspicious activity.
   - Reporting obligations and traceability of transactions: The directive requires all cryptocurrency transactions to be traceable in order to facilitate the tracing of potential illegal activities such as money laundering.
   - Greater transparency: greater transparency in the ownership of cryptocurrency-related companies and accounts is required to prevent the use of these funds for money laundering or terrorist financing.
3) The Whistleblower Directive (EU) 2019/1937: it offers an important framework for the protection of whistleblowers, including money laundering and cryptocurrency abuse. Businesses, including cryptocurrency businesses, are obliged to put in place whistleblowing mechanisms, which are important for the detection and prevention of crypto money laundering.
4) Regulation (EU) 2018/1724 on the European Anti-Money Laundering Regulation (EMD): it ensures the consistent implementation of AML/CFT legislation in the EU. It is a key legal framework that facilitates the exchange of information and ensures a uniform approach by EU Member States in the fight against money laundering, including the use of cryptocurrencies.
5) Markets in Crypto-Assets (MiCA): MiCA (Markets in Crypto-Assets) is a proposed regulatory framework that will introduce more specific rules for crypto markets in the EU. The aim is to create a single legal framework to prevent money laundering and terrorist financing in the crypto sector.

8.1. The Bank of Slovenia's powers

Article 3(48) of the Act on Prevention of Money Laundering and Terrorist Financing (ZPPDFT-2) defines virtual currency services as services provided by a natural or legal person as a business or profession to a third party: an exchange between fiat and virtual currencies, the transfer of virtual currencies between different accounts or addresses, the custody or management of virtual currencies, including the provision of private cryptographic key protection services on behalf of its clients, for the storage, safekeeping and transfer of virtual currencies, services relating to the issue or sale of virtual currencies (ZPPDFT-2, 2016). The Bank of Slovenia is also responsible for monitoring the consistent implementation of the obligations of virtual value service providers. On 9 June 2023, the Markets in Crypto-assets Regulation was published in the Official Journal of the European Union, which establishes uniform requirements for (Banka Slovenije, 2017) the

issuance, public offering and admission to trading on a trading platform of asset-linked tokens, e-money tokens that are neither asset-linked tokens nor e-money tokens; and cryptocurrency service providers (e.g. exchanging cryptocurrencies for cash). The provisions of the Regulation (EU) on cryptoasset markets on the conditions for issuing asset-linked tokens and e-money tokens apply from 30 June 2024, while the remaining provisions will apply from 30 December 2024 (Banka Slovenije, 2017).

8.2. Responsibilities of the Office for the Prevention of Money Laundering of the Republic of Slovenia

The Office for the Prevention of Money Laundering of the Republic of Slovenia (hereinafter referred to as the UPPD) is a body operating within the Ministry of Finance and is responsible for monitoring and preventing money laundering and terrorist financing in Slovenia. The UPPD is responsible for collecting data, analysing suspicious transactions and cooperating with other national and international institutions such as the Financial Intelligence Unit (FBI) and Europol (Republic of Slovenia, 2024). As virtual currency transactions take place in a virtual world and between individuals from different countries, traditional mechanisms for combating money laundering, terrorist financing and tax evasion are often not as effective as in the case of traditional transactions (Republic of Slovenia, Court of Auditors, 2019).

Slovenia has taken various measures to address the risks associated with the use of cryptocurrencies for illicit purposes (OpenAI, 2024):

1) Regulation of cryptocurrencies: Slovenia is part of the European framework for the regulation of cryptocurrencies, such as the EU legislation governing Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) guidelines. Cryptocurrencies are treated as a means of payment, which means that they have to be managed in accordance with AML requirements.
2) User identification: companies that facilitate cryptocurrency exchanges or provide other services related to cryptocurrencies are obliged to implement Know Your Customer (KYC) procedures, which include verifying the identity of users to prevent anonymous or illegal transactions.
3) Suspicious transaction reporting: under the legislation, companies trading in cryptocurrencies are obliged to report suspicious transactions and cooperate with money laundering investigations.
4) Cooperation with international institutions: Slovenia cooperates closely with other countries and international organisations such as the European Commission, the European Central Bank and other financial institutions to exchange information and coordinate measures to prevent cryptocurrency abuse.

9. CONCLUSION

Cryptocurrencies are an innovation that complements the traditional payment system. However, their anonymity, fast transactions and lack of regulatory frameworks have made them attractive vehicles for illicit activities such as money laundering. Money laundering with cryptocurrencies is one of the key threats posed by this technology, as it allows the rapid, often anonymous and cross-border transfer of funds. In practice, this means that individuals or organised criminal groups can use cryptocurrencies to »clean« illegally obtained money, allowing the conversion of illicit funds into apparently legitimate ones. This is possible due to the nature of cryptocurrencies, which often provide a degree of anonymity and harder-to-trace transactions compared to traditional banking systems.

The regulation of virtual currencies in the context of anti-money laundering is the European Union's first response to this issue. Although legislation in this area is still under development in Slovenia, measures have already been taken to better track and monitor transactions in the crypto world. In any case, further steps in the development of appropriate regulations and cooperation with international bodies will be crucial to prevent abuses and ensure the security of the financial system. In addition, it is important to raise public awareness of the risks associated with cryptocurrencies and to educate the public on how to avoid money laundering risks. Companies and individuals using cryptocurrencies need to be alert to potential illegal activities and adhere to regulatory guidelines to ensure that this technology remains a tool for innovation and progress, not a means for financial abuse. A comprehensive approach to regulation, aligned with international practices, will help protect Slovenia from the risks of using cryptocurrencies for illicit purposes.

References

Ashford, K. (2023). What is Cryptocurrency? Retrieved from https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/

Banka Slovenije. (2017). The Eurosystem. Frequently asked questions and answers on crypto-assets. Retrieved from https://www.bsi.si/placila-in-infrastruktura/pogosta-vprasanja-in-odgovori-o-kriptosredstvih

Bank for International Settlements. (2018). Annual economic report 2018. Retrieved from https://www.bis.org/publ/arpdf/ar2018e5.pdf

Becher, B. (2024). Blockchain: What It Is, How It Works, Why It Matters. Retrieved from https://builtin.com/blockchain

Constitution of the Republic of Slovenia. (1991). Official Gazette of the Republic of Slovenia, No. 33/91-I, 42/97 - UZS68, 66/00 - UZ80, 24/03 - UZ3a, 47, 68, 69/04 - UZ14, 69/04 - UZ43, 69/04 - UZ50, 68/06 - UZ121,140,143, 47/13 - UZ148, 47/13 - UZ90,97,99, 75/16 - UZ70a and 92/21 - UZ62a)

Copeland, T. (2023). What are different types of cryptocurrencies and tokens? Retrieved from https://www.theblock.co/learn/249518/what-are-the-different-types-of-cryptocurrencies-and-tokens

Criminal Code. (2012). Official Journal of the Republic of Slovenia, No. 50/12 - Official consolidated text, 54/15, 6/16 - corrected, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 - ZZNŠPP and 16/23)

Fang, F., Ventre, C., Basios, M., Kanthan, L., Martinez-Rego, D., Wu, F., & Li, L. (2022). Cryptocurrency trading: a comprehensive survey. Financial Innovation, 1.

FATF Report. (2014). Virtual Currencies - Key Definitions and Potential AML/CFT Risks. Retrieved from https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Fortuna, M. (2022). Cryptocurrency Mining: When will the last BTC be mined? Everything you need to know about mining! Retrieved from https://martinfortuna.si/rudarenje-kriptovalut/

Frankenfield, J. (2022). Ethereum. Investopedia. Retrieved from https://www.investopedia.com/terms/e/ethereum.asp

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014). Bitcoin - Asset or Currency? Revealing Users´ Hidden Intentions. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425247

Haegele, B. (2024). What is Coinbase and how does it work? Retrieved from https://www.bankrate.com/investing/what-is-coinbase/

IBM. (n.d.). Blockchain. IBM. Retrieved from https://www.ibm.com/topics/blockchain

International Monetary Fund. (2014). The IMF and the Fight Against Money Laundering and the Financing of Terrorism. Retrieved from https://www.imf.org/en/Topics/Financial-Integrity/amlcft

Lamberger, I. (2009). Economic Crime. Ljubljana: Faculty of Security Sciences.
Law on Prevention of Money Laundering and Terrorist Financing. (2016). (Official Journal of the Republic of Slovenia, No. 68/16, 81/19, 91/20, 2/21 - corrected and 48/22 - ZPPDFT-1, ZPPDFT-2).
Likos, P., & Hicks, C. (2022). The History of Bitcoin, the First Cryptocurrency, U.S. News & World Rep. Retrieved from https://money.usnews.com/investing/articles/the-history-of-bitcoin (reciting a history of bitcoin)
OpenAI. (2024). ChatGPT [Generative AI model]. Retrieved from https://chat.openai.com
Republic of Slovenia. (2024). Office for the Prevention of Money Laundering. Retrieved from https://www.gov.si/drzavni-organi/organi-v-sestavi/urad-za-preprecevanje-pranja-denarja/o-uradu/
Republic of Slovenia, Court of Auditors. (2019). Audit report. Retrieved from https://www.rs-rs.si/revizije-in-revidiranje/arhiv-revizij/revizija/ureditev-podrocja-virtualnih-valut-v-republiki-sloveniji-1704/
Republic of Slovenia, Ministrstvo za notranje zadeve. (2024). Online Fraud on the rise again, be careful Policija. Retrieved from https://www.policija.si/medijsko-sredisce/sporocila-za-javnost/sporocila-za-javnost-gpue/123181-porast-goljufij-na-spletu
Republic of Slovenia, Ministry of Internal Affairs. (2018). Seven types of online financial scams that users most often fall for, Police. Retrieved from https://www.policija.si/svetujemo-ozavescamo/varnost-na-internetu/sedem-vrst-spletnih-financnih-prevar-ki-jim-uporabniki-najpogosteje-nasedejo
Republic of Slovenia, Ministry of the Interior. (2022). The police are intensively investigating various forms of online fraud, which are still on the rise. Retrieved from https://www.policija.si/medijsko-sredisce/sporocila-za-javnost/sporocila-za-javnost-gpue/115985-policija-intenzivno-preiskuje-razlicne-oblike-spletnih-goljufij-ki-so-se-vedno-v-porastu
Rosen, A. (2024). Cryptocurrency Basics: Pros, Cons and How It Works. Retrieved from https://www.nerdwallet.com/article/investing/cryptocurrency
Safe on the Internet. (2024). Retrieved from https://www.varninainternetu.si/smishing-sms-sporocila-za-krajo-podatkov/
Šepec, M. (2023). In: Criminal Procedure Act (CPA): with commentary. 1st printing. Lexpera, GV publishing house
Suratkar, S., Shirole, M., & Bhirud, S. (2020). Cryptocurrency Wallet: A Review. 4th International Conference on Computer, Communication and Signal Processing (ICCCSP).
Vidrih, M. (2019). Decentralization - the power of the word you need to know. Retrieved from https://www.slovenec.org/2019/07/24/decentralizacija-moc-besede-ki-jo-morate-poznati/
Viitaharju, V. (2024). How do Bitcoin transactions work? Retrieved from https://www.northcrypto.com/learn/blog/how-do-bitcoin-transactions-work
World Bank Group. (2017). International Bank for Reconstruction and Development: Distributed Ledger Technology (DLT) and Blockchain. Retrieved from http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WPPUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf
Žaberl, M., Pozderec, F., & Oberman, I. (2017). Threat prevention as a basis for the exercise of security powers. Security Studies [online]. 2017. Vol. 19, no. 3, p. 273-292