CRYPTOCURRENCY REGULATION IN THE US AND THE CZECH REPUBLIC: A COMPARATIVE ANALYSIS OF ENFORCEMENT AND EFFECTIVENESS*

Tomáš Brandejský[a]

Abstract

The article *"Cryptocurrency Regulation in the US and the Czech Republic: A Comparative Analysis of Enforcement and Effectiveness"* examines the regulatory frameworks in both countries as they address the rising risks of fraud associated with crypto-assets like cryptocurrencies and Non-Fungible Tokens (NFTs). The United States adopts a proactive approach, leveraging multi-agency cooperation and existing legal frameworks to regulate this space, whereas the Czech Republic takes a more conservative stance, awaiting the implementation of EU regulations, notably the Markets in Crypto-Assets (MiCA). This comparative study highlights the strengths and weaknesses of both systems. The U.S. regulatory environment is characterized by adaptability and advanced enforcement tools such as blockchain analytics, but suffers from overlapping authorities and inconsistent legal interpretations. The Czech Republic, though still developing its legal framework, has demonstrated competence in seizing and monetizing fraudulently obtained crypto-assets, although its response times to fraud cases are slower. The article concludes by offering recommendations for the Czech Republic to enhance its regulatory framework, including adopting investigative methods from the U.S. and acting more proactively in the fight against crypto-related fraud. This analysis contributes to the ongoing debate on how to best regulate emerging financial technologies in this rapidly evolving market.

Keywords:

cryptocurrency regulation, NFT fraud, comparative analysis, enforcement effectiveness, MiCA Regulation, blockchain analytics, investor protection

JEL Classification: K24, K42, G28

1. Introduction

As crypto-assets, i.e. cryptocurrencies and Non-Fungible Tokens (NFTs), gradually become part of the global financial system, the risk of an investor becoming a victim of fraud also increases.[1,2] The United States and the Czech Republic are therefore developing regulatory frameworks to address these issues, but their approaches differ significantly. The United States

* The article was written as part of the IGS grant project "*Prevention of Crypto Asset Fraud and Failure of Related Service Providers in an International Context*" at the Prague University of Economics and Business, where the author, Mgr. Tomáš Brandejský, is a third-year PhD student.

a Prague University of Economics and Business

1 Kshetri, N. (2022). Scams, Frauds, and Crimes in the Nonfungible Token Market. Computer, 55(4), 60-64. https://doi.org/10.1109/MC.2022.3144763

2 Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11(1). https://doi.org/10.1186/s40163-021-00163-8

has adopted a proactive strategy based on multi-agency cooperation and has creatively adapted existing legal frameworks to cryptoassets, while the Czech Republic is more or less waiting for harmonisation at EU level and is very cautious about applying existing financial law rules to cryptoassets. As part of the harmonisation process, the Czech government has submitted a draft Digital Finance Act[3], which is intended to implement EU regulations in the area of digital finance, namely the *Digital Operational Resilience Act* (DORA)[4] on digital operational resilience of the financial sector, which applies to cryptoasset service providers, among many other entities, and the *Markets in Crypto Assets* (MiCA)[5] regulation on cryptoasset markets, but which does not apply to NFTs. The relevant parliamentary print is in its second reading at the time of writing.

The Czech Republic and the USA were chosen for this comparative analysis due to the stark contrast in their approaches to cryptocurrency regulation and enforcement. The United States has taken a proactive stance, adapting existing legal frameworks and employing multi-agency cooperation to address the challenges posed by cryptocurrencies and NFTs. In contrast, the Czech Republic has adopted a more conservative approach, largely awaiting the implementation of EU regulations, such as MiCA.

The main purpose of this comparison is to assess which country has a better regulatory approach, with the assumption that the US model offers valuable lessons for the Czech Republic. By analyzing the strengths and weaknesses of each system, the article aims to provide guidance to the Czech legislator on how to improve their regulatory framework and enforcement mechanisms in the rapidly evolving cryptocurrency market.

Although there is a sufficient amount of literature on US law and the procedures of US authorities in dealing with cryptocurrency fraud[6,7,8,9], similar literature focusing on Czech law and the procedures of Czech authorities is noticeably lacking. Nor is there any comparative analysis between the Czech and US approaches. Given that the US authorities arguably have

---

3 Chamber of Deputies of the Parliament of the Czech Republic (2024, 3 May). *Draft Act on the Digitization of the Financial Market*. Parliamentary Print 692. https://www.psp.cz/sqw/historie.sqw?o=9&T=692.

4 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience in the financial sector ("**DORA Regulation**") is effective from 16 January 2023. From this date, obliged entities have 24 months to reflect the new rules in their processes.

5 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets for cryptoassets ("**MiCA Regulation**") is applicable from 30 June 2023 and will become applicable in its entirety from 30 December 2024.

6 Saha, S., Ahmed Rizvan Hasan, Mahmud, A., Ahmed, N., Parvin, N., & Hemal Karmakar. (2024). Cryptocurrency and financial crimes: A bibliometric analysis and future research agenda. *Multidisciplinary Reviews*, 7(8), 2024168-2024168. https://doi.org/10.31893/multirev.2024168

7 Trozze, A., Davies, T., & Kleinberg, B. (2022). Explaining prosecutorial outcomes for cryptocurrency-based financial crimes. *Journal of Money Laundering Control*. https://doi.org/10.1108/jmlc-10-2021-0119.

8 Dimitris Kafteranis, Huseyin Unozkan, & Umut Turksen. (2023). COMPLIANCE AND ENFORCEMENT CHALLENGES IN TRADING OF NON-FUNGIBLE TOKENS. *International Journal of Law in a Changing World*, 2(3), 18-51. https://doi.org/10.54934/ijlcw.v2i3.57

9 Nolasco Braaten, C., & Vaughn, M. S. (2019). Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions. *Deviant Behavior*, 42(8), 1-21. https://doi.org/10.1080/01639625.2019.1706706

the most experience in this area due to the size of their crypto market as well as their proactive enforcement approach, a comparison of these approaches could offer valuable insights for improving Czech regulatory practice.

This article therefore seeks to compare the current legislation and enforcement approaches to cryptoasset fraud in the Czech Republic and the United States. Through the method of comparative analysis, the article will explore the strengths and weaknesses of the respective legislation and assess the approach of the authorities in each country to cryptocurrency fraud. By understanding these differences, the article aims to identify possible recommendations for Czech practice. Ultimately, then, this analysis aims not only to highlight the successes and failures of the two countries under review, but also to offer guidance on how the Czech Republic can improve its regulatory framework to more effectively address the ever-evolving fraudulent schemes in the cryptoasset market.

2. US legal environment

In the United States, the responsibility for regulating and overseeing the cryptocurrency market is divided between federal and state authorities. At the federal level, the Securities and Exchange Commission (SEC)[10], the Commodity Futures Trading Commission (CFTC)[11], and the Department of Justice (DOJ)[12] oversee the cryptoasset market based on whether a particular cryptoasset is classified as a security, a commodity, or whether a crime has been committed in connection with the cryptoasset. The Financial Crimes Enforcement Network (FinCEN)[13] ensures compliance with anti-money laundering (AML) regulations, while the Internal Revenue Service (IRS)[14] oversees the taxation of cryptoasset profits.

Under the Supremacy Clause of the U.S. Constitution[15], if state laws conflict with federal laws, federal laws prevail.[16] However, in areas where federal law is silent, such as business licensing, states can enact their own regulations. On this basis, some states have imposed strict licensing requirements on cryptocurrency businesses, such as New York with its BitLicense legislation[17], while in contrast, for example, Wyoming takes a much more accommodating, "crypto-friendly" stance[18]. Thus, while the SEC may, for example, regulate whether an NFT is a security or a derivative, states may impose additional requirements on how businesses

10 U.S. Securities and Exchange Commission ("**SEC**" or "**Securities Commission**")

11 Commodity Futures Trading Commission ("**CFTC**")

12 United States Department of Justice ("**DOJ**")

13 Financial Crimes Enforcement Network ("**FinCEN**")

14 Internal Revenue Service ("**IRS**")

15 U.S. Constitution ("**U.S. Constitution**"), Article VI, Clause 2

16 Susan Low Bloch, & Jackson, V. *Federalism: a reference guide to the United States Constitution*. Praeger, An Imprint Of Abc-Clio, Llc.

17 Baker, B. (2017). Application of the New York BitLicense to Initial Coin Offerings. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3319540

18 Andhov, A. (2021). Wyoming's Wild West Blockchain Laws and a Start-up Lobby. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3898451

operate within their jurisdiction. This dual system requires companies and individuals to know and comply with both federal and state laws, creating a complex and difficult regulatory environment.

2.1 Cryptoassets as securities

Federal securities regulation, which is primarily contained in the Securities Act[19] and the Securities Exchange Act[20], applies to cryptoassets if they meet the criteria of the so-called Howey test[21]. The Howey test assesses whether investors are entering into an *investment contract* when they buy cryptoassets, i.e. whether they are investing money in a *common enterprise* with the expectation of a profit generated primarily from the efforts of others. The most important cryptocurrencies, such as bitcoin and ether, are not considered securities by the Securities Commission, mainly because they are decentralised (i.e. not controlled by a single entity). While investors buy bitcoin and ether for profit, they do not expect to profit from the efforts of other persons, but from an increase in price, mainly based on higher market demand in the future.[22] In contrast, the cryptocurrency Ripple (XRP) is a security according to the SEC, as are many other cryptoassets issued in fundraising.[23]

However, the unique characteristics of cryptocurrencies, such as decentralization and technological complexity, challenge the traditional notions of investment contracts and the roles of promoters and investors. Some legal scholars and industry experts argue that the Howey test, developed in a vastly different economic and technological context, may not be adequately equipped to assess the nuances of cryptocurrency investments. They contend that applying a nearly century-old test to a nascent and rapidly evolving technology like cryptocurrencies could lead to misinterpretations and hinder innovation.

The Securities Act requires that, if a cryptoasset is a security, the *initial coin offering* (ICO) must be registered in advance as an offering of the security with the SEC and disclosures must be made to potential investors. The Securities Exchange Act then regulates the sale of securities and other information and reporting obligations. In addition, it also contains Rule 10(b) and Rule 10b-5, which prohibit fraud, market manipulation and insider trading in the trading of securities.

Enforcement of these rules is the responsibility of the Securities and Exchange Commission, which has the power to investigate and bring actions against persons involved in fraudulent schemes or unregistered securities offerings and is very active in doing so (see the list

19 Securities Act of 1933, 15 U.S.C. § 77a et seq. (1933).

20 Securities Exchange Act of 1934, 15 U.S.C. § 78a et seq. (1934).

21 U.S. Supreme Court (n.d.). *SEC v. Howey Co., 328 U.S. 293 (1946)*. Justia Law. https://supreme.justia.com/cases/federal/us/328/293/

22 *SEC Declares Bitcoin and Ether as Non-Securities*. (n.d.). Cassels. https://cassels.com/insights/sec-declares-bitcoin-and-ether-as-non-securities/

23 SEC.gov | *SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering*. (2020). Sec.gov. https://www.sec.gov/newsroom/press-releases/2020-338

on the SEC's dedicated website at[24]). To this end, the SEC has several powers, including the ability to initiate a court order to cease and desist or freeze assets or impose civil penalties for securities law violations in federal court. However, the SEC often resolves these cases through settlements in which the fraudsters voluntarily agree to pay a fine and comply with the rules *pro futuro*, which provides immediate remedies without the need to go to trial. For example, BlockFi agreed to a $100 million settlement for failing to register its crypto lending product in advance.[25] This was one of the largest settlements in a cryptocurrency-related enforcement action. The Securities and Exchange Commission also operates the so-called FinHub (Office of Strategic Hub for Innovation and Financial Technology), where it works with entrepreneurs and financial technology developers to find a rational way to regulate the cryptocurrency market.[26] In addition, the SEC has a whistleblowing program that encourages people with information about fraudulent schemes to cooperate by sharing in the seizure of funds (10 to 30%)[27]. For investors, the SEC has created a cryptoasset information page[28], which also includes a description of the most common ways that fraudsters try to defraud those interested in investing in cryptoassets. [29]

2.2 Cryptoassets as commodities and their derivatives

The Commodity Futures Trading Commission (CFTC) regulates the derivatives market (futures, options and swaps), including derivatives based on crypto-assets, under the Commodity Exchange Act[30] . Thus, the CFTC's authority extends only to crypto-assets that are considered commodities, including, for example, bitcoin and ether.[31] Although the CFTC generally does not oversee the spot market for commodities (where commodities are sold without delay), its jurisdiction also extends to fraud and market manipulation in the spot market for commodities.

24 *Crypto Assets*. (n.d.). Sec.gov; U.S. Securities and Exchange Commission. https://www.sec.gov/securities-topics/crypto-assets

25 SEC.gov | *BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product*. (n.d.). Www.sec.gov. https://www.sec.gov/newsroom/press-releases/2022-26

26 SEC.gov | *Office of Strategic Hub for Innovation and Financial Technology (FinHub)*. (2023). Sec.gov. https://www.sec.gov/about/divisions-offices/office-strategic-hub-innovation-financial-technology-finhub

27 SEC.gov | *Whistleblower Program*. (n.d.). Sec.gov. https://www.sec.gov/enforcement-litigation/whistleblower-program

28 *Crypto Assets*. (n.d.-b). Investor.gov; U.S. Securities and Exchange Commission. https://www.investor.gov/additional-resources/spotlight/crypto-assets

29 *5 Ways Fraudsters May Lure Victims Into Scams Involving Crypto Asset Securities - Investor Alert*. (2024). Investor.gov; U.S. Securities and Exchange Commission. https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/crypto-scams

30 Commodity Exchange Act of 1936, 7 U.S.C. § 1 et seq. (1936).

31 Davis, D., & Kim, A. (2024, July 9). *Ether's Legal Status Clarified? CFTC Scores Win as Court Backs Agency's Commodity Classification*. Katten. https://quickreads.ext.katten.com/post/102jcc8/ethers-legal-status-clarified-cftc-scores-win-as-court-backs-agencys-commodity#page=1

Notable CFTC cases include actions against prominent cryptocurrency exchanges such as Binance, FTX and Coinbase.[32] The CFTC also frequently publishes warnings about common cryptocurrency fraud schemes or motivates potential whistleblowers by offering financial rewards. To detect suspicious transactions, the CFTC uses, among other things, analysis of market activity in commodities markets. Similar to the SEC, the CFTC has created an initiative to work with the private sector on fintech and cryptoassets, called LabCFTC. Thus, it can be concluded that the CFTC is able to apply to cryptoasset fraud without much difficulty even legislation that was enacted before the emergence of cryptoassets.

2.3 Criminal dimension of cryptoasset fraud

The Department of Justice (DOJ) and its principal investigative arm, the Federal Bureau of Investigation (FBI), are responsible for criminal enforcement related to cryptocurrency and NFT fraud[33]. Cryptocurrency fraud is prosecuted primarily as wire fraud[34], i.e., fraud committed through communications technology. However, these cases are often linked to money laundering charges. Prosecution can lead to imprisonment, fines or confiscation of assets. While the SEC and CFTC may bring civil actions for violations of securities or commodities market rules (e.g., failure to register a securities offering), the Department of Justice focuses on crimes that intentionally cause fraud or harm. It is not uncommon for a single fraudulent scheme to be simultaneously prosecuted by both the DOJ (e.g., as wire fraud) and the Securities Commission for violations of securities trading rules. As a result, these agencies often coordinate their efforts, share information, and sometimes even conduct joint investigations.[35]

The Department of Justice also established a Crypto Enforcement Unit in 2019 that specializes in prosecuting cryptocurrency fraud. In addition to standard legal tools, prosecutors also use blockchain data analysis to identify and prosecute complex fraud schemes and cases of market manipulation.[36]

The DOJ's work is particularly critical in large-scale cases like OneCoin and BitConnect, where fraudsters have bilked investors out of billions of dollars. The DOJ has also been successful in tracing and seizing cryptoassets related to criminal activity. For example,

32 *CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange* | CFTC. (n.d.). Www.cftc.gov. https://www.cftc.gov/PressRoom/PressReleases/8680-23

33 Federal Bureau of Investigation ("**FBI**")

34 Wire fraud is a federal crime that involves the use of an electronic communication, such as the Internet, email, or telephone, to intentionally deceive a third party and enrich oneself at that person's expense. In the case of cryptocurrency fraud, it often involves phishing scams, Ponzi schemes, and fake investment opportunities offered online.

35 Allen, B., Brez, Z., Kalil, C., Kasulis, J., & Mouritsen, S. (2024). *DOJ and SEC crypto exchange enforcement in the United States*. Globalinvestigationsreview.com. https://globalinvestigationsreview.com/review/the-investigations-review-of-the-americas/2025/article/doj-and-sec-crypto-exchange-enforcement-in-the-united-states

36 *Criminal Division | Crypto Enforcement*. (2022, July 5). Justice.gov. https://www.justice.gov/criminal/criminal-fraud/crypto-enforcement

the tracing and seizure of a significant portion of the ransom (a total of 63.7 bitcoins worth $2.3 million) paid by Colonial Pipeline Co. as ransom in connection with the most serious ransomware attack in the U.S. to date, which led to fuel shortages throughout the East Coast.[37]

2.4 Strengths and weaknesses

The strengths of the U.S. approach undoubtedly include a proactive enforcement approach and the use of new technologies and advanced data analytics to detect fraudulent activity. US regulators are also known for cracking down on cryptocurrency fraud regardless of the nationality of the perpetrators. They base their jurisdiction on the often hypothetical argument that fraudulent activity also affects US citizens, without identifying the specific citizens involved.[38] Critics of this approach rationally point out that these are only U.S. regulators, not global surveillance organizations. On the other hand, the global approach of the US authorities is to be welcomed, as their actions ultimately protect the citizens of other countries and compensate for any inaction by their national authorities.

In any case, the US legal system offers a robust basis for dealing with cryptocurrency fraud. These include the Securities Act, the Securities Exchange Act and the Commodity Exchange Act. The relevant provisions allow for broad interpretation, giving regulators the chance to adapt to the evolving nature of cryptoassets.

The way in which the US authorities try to inform the public about the risks and the efforts to establish cooperation with whistleblowers through economic motivation can also be appreciated. Another strength of the American approach is definitely interinstitutional cooperation. Cooperation between different regulatory authorities (SEC, DOJ, CFTC, FinCEN) ensures that different aspects of the market are covered, from securities and commodities regulation to anti-money laundering efforts. This approach allows for comprehensive oversight of both the cryptocurrency and NFT markets.[39]

On the other hand, the US approach to cryptocurrency fraud has its weaknesses. The involvement of multiple authorities invariably brings with it overlapping powers and inconsistent interpretation of regulations, which can confuse market participants and deter legitimate businesses from entering the market. Examples include exchanges such as Coinbase and Binance, which have faced lawsuits from both the SEC and the CFTC.[40] Inconsistent interpretation can also sometimes lead to loopholes in the law that fraudsters can exploit. Thus, while

37 Bing, C. (2021, June7). *U.S. seizes $2.3 million in bitcoin paid to Colonial Pipeline hackers*. Reuters. https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/.

38 For the first time, U.S. courts did so with respect to cryptoassets in SEC v. Traffic Monsoon, LLC, 245 F. Supp. 3d 1275 (D. Utah 2017).

39 Tan, C. (2024). Rights in NFTS and the flourishing of NFT marketplaces. *International Journal of Law and Information Technology*, 32(1). https://doi.org/10.1093/ijlit/eaae018

40 O'Melveny & Myers LLP. (2024, October 18). *The Ever-Shifting Landscape of U.S. Crypto Regulation*. OMM.com. https://www.omm.com/insights/alerts-publications/the-ever-shifting-landscape-of-us-crypto-regulation/

U.S. regulators have been proactive in enforcing the law, the regulatory environment still has some room for improvement.

While the SEC has taken a strong stance against certain cryptocurrency projects and individuals, some critics argue that their enforcement actions have not always been consistent or effective. For example, the SEC has been criticized for its handling of the Ripple (XRP) case, with some arguing that the agency overstepped its authority and caused unnecessary harm to investors. The SEC has also been accused of being slow to act in cases of alleged fraud, such as the BitConnect scheme, which operated for over a year before facing regulatory action.

Furthermore, the SEC's support of Sam Bankman-Fried, the founder of the now-defunct FTX exchange, has raised questions about the agency's judgment and its potential susceptibility to influence. Bankman-Fried was a vocal advocate for cryptocurrency regulation and a major donor to political campaigns, and some critics argue that this may have influenced the SEC's favorable treatment of him and his company. The collapse of FTX, which was once one of the largest cryptocurrency exchanges in the world, has also cast a shadow over the US regulatory landscape. The company's implosion, which resulted in billions of dollars in losses for investors, exposed significant weaknesses in the US regulatory framework and raised questions about the ability of regulators to effectively oversee the cryptocurrency market.

These criticisms highlight the challenges and complexities of regulating the cryptocurrency market, even in a country with a well-developed legal system like the United States. While the US has been a leader in cryptocurrency regulation, there is still room for improvement in terms of consistency, effectiveness, and the ability to adapt to the rapidly evolving nature of the market.

3. Legal environment in the Czech Republic

The Czech legislation on crypto-assets is much more stringent than the American one. Cryptoassets do not yet have a comprehensive legal framework in the Czech Republic, although this will change to a large extent once the MiCA regulation[41] and hopefully adaptive legislation comes into force. On the other hand, it cannot be said that cryptoassets are in a legal vacuum either.

Crypto-assets are not considered money, currency or commodity in the Czech Republic, yet in the sense of Section 489 of the Civil Code[42] they are things in the legal sense, namely intangible, movable and fungible. In the case of NFTs, it is usually an unrepresentable thing. Crypto-assets are not even a commodity under the Commodity Exchange Act because they do not have a tangible substance. Czech law also does not recognise digital securities other than book-entry securities. In some cases, however, cryptoassets may meet the definition of electronic money under the Payment Act. The first defining characteristic of electronic money is that it is a monetary value that represents a claim against the issuer. This definition is met in particular by some stablecoins, whose value is typically pegged to official currencies

41 The MiCA portion of the regulation took effect on June 30, 2024, and the full regulation willtake effect on December 30, 2024.

42 Act No. 89/2012 Coll., Civil Code, as amended.

such as USD or EUR. However, cryptocurrencies are accepted as a legitimate form of payment and the Czech National Bank does not restrict their use in any way.[43] However, the provision of services related to virtual assets is a free trade under the Trade Act, which, subject to the general conditions (legal capacity, integrity), only needs to be declared.[44]

Some cryptoassets may also meet the definition of an investment instrument under the Capital Market Enterprise Act[45]. For example, if they are derivatives or foreign cryptoassets that are investment securities under foreign law.[46]

Thus, crypto-assets are specifically regulated by the AML Act[47]. A virtual asset is an electronically storable or transferable unit that is capable of performing a payment, exchange or investment function, regardless of whether it has an issuer or not [Section 4(9) of the AML Act]. Both cryptocurrencies and NFTs meet this definition. A payment by a virtual asset has the same treatment as a cash payment in terms of the AML Act [Section 54(5) of the AML Act]. Therefore, natural persons and legal entities making a payment with a virtual asset exceeding EUR 10,000 are considered to be obliged persons under the AML Act. Providers of services related to virtual assets are also obliged to be obliged and must therefore, for example, identify their clients and carry out suspicious transaction analysis (Article 2(1)(l) of the AML Act).[48]

Czech criminal law does not explicitly address crypto-assets. The only exception is the criminal offence of unauthorised provision, forgery and alteration of a means of payment, which mentions means of payment that allow the withdrawal or transfer of virtual assets used instead of cash [Article 234(1) of the Criminal Code[49]]. Nevertheless, crypto-assets, as things of a certain economic value, can be subject to criminal offences, typically those of property, in particular theft or embezzlement[50]. A significant problem is, as in the US, the use of crypto-assets to launder the proceeds of crime. It should also not be forgotten that any profits from crypto-assets must be taxed or the offence of evasion of tax, duty or similar payment may be committed. Seized cryptoassets are then sold by the state as early as 2021 through the Office for State Representation in Property Matters, and in 2024 the state is expected to make

43 Spilka, D. (2023, May 16). *What does the adoption of cryptocurrencies in the Czech Republic mean from a legal perspective?* Legal Space. https://www.pravniprostor.cz/clanky/financni-pravo/co-znamena-prijeti-kryptomen-v-ceske-republice-z-pravniho-hlediska.

44 Act No. 455/1991 Coll., on trade business (Trade Licensing Act), as amended.

45 Act No. 256/2004 Coll., on Capital Market Business, as amended.

46 *On the possibility for investment funds to invest in cryptoassets* (2021). Czech National Bank. https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/stanoviska-k-regulaci-financniho-trhu/RS2023-05/.

47 Act No. 253/2008 Coll., on Certain Measures against the Legalization of the Proceeds from Crime and the Financing of Terrorism, as amended (the "**AML Act**").

48 Plecitý, D. (n.d.). AML REGULATION: Cryptocurrencies and laundering of proceeds of crime. *Bankingonline.cz*. Retrieved October 19, 2024, from https://fau.gov.cz/files/kryptomeny-a-legalizace-vynosu-z-trestne-cinnosti.pdf

49 Act No. 40/2009 Coll., the Criminal Code, as amended (hereinafter referred to as the "**Criminal Code**").

50 CTK. (2019, September5). *Court reconsiders bitcoin theft to embezzlement, programmer gets 9 years*. IDNES.com. https://www.idnes.cz/brno/zpravy/soud-programator-tomas-jirikovsky-bitcoiny-zpronevera.A190905_121842_brno-zpravy_krut

approximately CZK 100 million (USD 4.3 million) from the sale of cryptoassets.[51] In addition, the police issued a methodology for seizing cryptocurrencies back in 2014, which was updated in 2019.[52]

The Czech Republic's new Digital Finance Act (Act No. 31/2025 Coll.), which implements the EU's MiCA regulation, is accompanied by a separate Amendment Act (Act No. 32/2025 Coll.). This Amendment Act introduces a time and value test to determine the tax liability for individuals investing in cryptoassets. The time test exempts profits from the 15% tax if investors hold cryptocurrencies for at least three years. This exemption is retroactive, applying to cryptocurrencies held three years before the law's enactment, potentially allowing tax-free sales as early as the beginning of 2025. The value test exempts income from the sale of cryptoassets up to CZK 100,000 per tax year, simplifying tax obligations for small transactions. Additionally, an aggregate exemption applies to income up to CZK 40 million, with any excess being taxed. These provisions are found in Sections 4(zj), 4(zk) and 4(3) of the Amendment Act. This law was promulgated in the Collection of Laws on 14 February 2025 and is effective from 15 February 2025.

4. Case studies

4.1 OneCoin

OneCoin, which operated between 2014 and 2017, was a fraudulent scheme masquerading as a legitimate investment in the eponymous crypto asset. Marketed since 2014 as "The Bitcoin Killer," ready to revolutionize the financial system, OneCoin coins were in fact worthless. It is estimated that 3.5 million people worldwide have fallen victim to the scam, losing more than $4 billion in total. The OneCoin scam is thus one of the biggest scams in human history.[53] The scheme gained the most investors between 2015 and 2016. Ruja Ignatova, a German businesswoman of Bulgarian origin, known as "Cryptoqueen" was behind the scheme. She collaborated with a Swede, Karl Sebastian Greenwood, who managed the project through OneCoin Ltd and OneLife Network Ltd, registered in Dubai and Belize respectively.[54]

OneCoin operated as a global Ponzi scheme, paying out funds to early investors from newer ones and using a multi-level marketing (MLM) strategy to recruit investors. Investors received commissions for recruiting others, creating a pyramid-like structure. Unlike legitimate cryptocurrencies and official prospectuses, OneCoin coin transactions were not recorded on a decentralized blockchain. Transactions were simulated within a closed system with

51 Kateřina Vaníčková. (2024, May4). *The state sends over 4 bitcoins to the auction, the starting price exceeds CZK 6 million*. IDNES.cz. https://www.idnes.cz/zpravy/domaci/stat-majetek-prodej-virtualni-mena-miliony-korun-bitcoin-aukce.A240504_103127_domaci_vank

52 Fischer, J. (2024). *Reflection of cryptocurrencies in selected areas of criminal law* [Master's thesis (Mgr.)]. https://theses.cz/id/7tpslf/

53 Zhang, A. R., Raveenthiran, A., Mukai, J., Naeem, R., Dhuna, A., Parveen, Z., & Kim, H. (2019). The Regulation Paradox of Initial Coin Offerings: A Case Study Approach. *Frontiers in Blockchain*, 2. https://doi.org/10.3389/fbloc.2019.00002

54 Innocent Chiluwa. (2019). "Truth," Lies, and Deception in Ponzi and Pyramid Schemes. *IGI Global EBooks*, 439-458. https://doi.org/10.4018/978-1-5225-8535-0.ch023

no mining or other mechanism to guarantee the authenticity of the data. The company also arbitrarily determined and falsely inflated the value of the coin, creating the illusion of growth. There was no real market or independent exchange for trading OneCoin. Although OneCoin promoted its internal exchange, xcoinx, it was often out of service, making it impossible for investors to cash out their purported profits. OneCoin coins could not be purchased directly. Instead, "educational packages" on cryptocurrency trading were sold, which included tokens redeemable for OneCoin coins. The prices of these packages ranged from several hundred to tens of thousands of euros.[55]

Since the beginning of 2016, the media began to write about the suspected fraudulent nature of the OneCoin project.[56] Authorities in several countries have issued warnings, launched investigations and taken further legal action against OneCoin and its promoters. Authorities in Bulgaria were the first to investigate the project in 2015.[57]

The mastermind of the scam, Ruja Ignatova, disappeared in late October 2017 after a secret arrest warrant was issued for her in the US. Although she has been on the FBI's Ten Most Wanted List since June 2022 and the reward for information leading to her arrest has been increased to $5 million, she remains at large, as long as she is alive.[58] Ignatova is facing securities fraud and money laundering charges in the US. Her brother Konstantin Ignatov, who took over the project, was arrested in the US in 2019 and is cooperating with authorities. Co-founder Karl Sebastian Greenwood was arrested in Thailand in 2018 and extradited to the US, where he was sentenced to 20 years in prison for financial fraud in 2023.[59] US lawyer Mark Scott was sentenced to 10 years in prison in 2019 for laundering $400 million of OneCoin's proceeds.[60] In China, authorities seized approximately $250 million and convicted 33 people in connection with the fraud.[61]

---

55 Bartlett, J. (2023). *The Missing Cryptoqueen*. Ebury Publishing.

56 Penman, A. (2016, February 10). *Here's why hyped-up web currency OneCoin is virtually worthless*. The Mirror. https://www.mirror.co.uk/news/uk-news/who-wants-onecoin-millionaire-you-7346558

57 *NOTICE - OneCoin - Financial Supervision Commission*. (2015, September 30). Financial Supervision Commission. https://www.fsc.bg/saobshtenie-onecoin/

58 *Up to $5 Million Reward Offer for Information Leading to Arrest and/or Conviction of Cryptocurrency Fraudster Ruja Ignatova*. (2024). United States Department of State. https://www.state.gov/up-to-5-million-reward-offer-for-information-leading-to-arrest-and-or-conviction-of-cryptocurrency-fraudster-ruja-ignatova/

59 *Co-Founder Of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced To 20 Years In Prison*. (2023, September 12). Justice.gov; U.S. Attorney's Office, Southern District of New York. https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison

60 *Former Law Firm Partner Sentenced To 10 Years In Prison For Laundering $400 Million Of OneCoin Fraud Proceeds*. (2024, January 25). Justice.gov; U.S. Attorney's Office, Southern District of New York. https://www.justice.gov/usao-sdny/pr/former-law-firm-partner-sentenced-10-years-prison-laundering-400-million-onecoin-fraud

61 Yang, Y. (2018, May 29). *China prosecutes 98 people, recovers US$268 million in OneCoin cryptocurrency investigation, report says*. SCMP.com; South China Morning Post. https://www.scmp.com/tech/article/2148114/china-prosecutes-98-people-recovers-us268-million-onecoin-cryptocurrency

4.2 BitConnect

The UK investment platform BitConnect was established in February 2016. Investors could buy BitConnect Coin (BCC) cryptocurrency for bitcoin and lend it back to the platform to run a trading bot with a promised return of up to 40% per month. The trading bot reportedly generated profits using arbitrage software that exploited fluctuations in the price of BTC. The platform also incentivized investors to recruit new members through a multi-level MLM system with commissions of up to 7%.[62]

In reality, BitConnect operated as a Ponzi scheme, using funds from newer investors to pay returns to earlier investors. Only a small portion of the funds from investors were used for arbitrage, most were transferred to the wallets of the scheme participants. Founder Satish Kumbhani and his associates raised approximately $2.4 billion through the scheme. They also manipulated the price of the BCC token to create the appearance of high market demand. The scheme began to unravel in late 2017 and early 2018. In January 2018, regulators in Texas and North Carolina banned BitConnect from operating because, in their view, BCC was an unregistered security and, in addition, BitConnect was not licensed to sell securities.[63,64] This led to the closure of the platform.

BitConnect eventually began offering investors payouts only in BCC tokens instead of bitcoin, which led to a loss of investor confidence and caused the token price to plummet from $525 to less than $1. Until then, BCC was among the top 20 most valuable cryptocurrencies. This collapse highlighted the risks associated with such investment platforms and triggered increased scrutiny from regulators. Eventually, BitConnect's founders and main promoters in the US were accused of running a Ponzi scheme and manipulating the market.

The Securities and Exchange Commission concluded that this was a fraudulent and unregistered sale of securities. This violated Sections 5(a), 5(c) and 17(a) of the Securities Act and Section 10(b) of the Securities Exchange Act. BitConnect also violated its obligation to register as a broker under Section 15(a) of the Securities Exchange Act. Act.[65] In terms of criminal law, so far only one of the main promoters of BCC in the US, Mr. Glenn Arcano, has been convicted and sentenced to USD 17 million in victim restitution for his involvement in the fraud.[66]

62 Chohan, U. (2018). Bitconnect and Cryptocurrency Accountability. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3131512

63 *$4 Billion Crypto-Promoter Ordered to Halt Fraudulent Sales*. (2022). Texas.gov; Texas State Securities Board. https://ssb.texas.gov/news-publications/4-billion-crypto-promoter-ordered-halt-fraudulent-sales

64 Emergency Cease and Desist Order (BitConnect), (Texas State Securities Board, Jan. 4, 2018). https://www.ssb.texas.gov/sites/default/files/BitConnect_ENF-18-CDO-1754.pdf

65 Complaint against BitConnect, Satish Kumbhani, Glenn Arcaro, and Future Money Ltd, (U.S. Securities and Exchange Commission, September 1, 2021). https://www.sec.gov/files/litigation/complaints/2021/comp-pr2021-172.pdf

66 *Crypto Fraud Victims Receive Over $17 Million in Restitution from BitConnect Scheme*. (2023, Jan. 12). Justice.gov; Office of Public Affairs. https://www.justice.gov/opa/pr/crypto-fraud-victims-receive-over-17-million-restitution-bitconnect-scheme

4.3 Insider Trading

So far, there are two known prosecutions of insider trading in the cryptocurrency market.[67] The first ever convicted is Nathanial Chastain, a former OpenSea manager who received a three-month prison sentence in May 2023 for buying NFT collections before they were advertised on the main page of the largest NFT marketplace. He was convicted of fraud and money laundering. Chastain was responsible at OpenSea for selecting the NFT collections to be displayed on the main site. Shortly before that, he bought them and then sold them at a multiple profit. After the promotion, interested parties were usually willing to pay a higher price, not only for the NFTs advertised, but also for other NFTs by the same author. To conceal his fraudulent conduct, Chastain used an anonymous digital wallet and anonymous OpenSea accounts for transactions. In addition to the prison sentence, Chastain also received three months of house arrest, three years of supervision, 200 hours of community service, a $50,000 fine, and an obligation to return the 15.98 ether coins he obtained in this manner (worth approximately $50,000).[68] This case is considered groundbreaking, although Chastain was not convicted directly for insider trading, as this can only be committed when trading in traditional financial instruments. Interestingly, the state authorities started investigating the case following a tip from an ordinary user who noticed suspicious transactions on the public blockchain.[69]

The second case is related to the well-known Coinbase exchange. Its former product manager, Ishan Wahi, was sentenced in May 2023 to two years in prison for wire fraud because he shared confidential information with his brother and his friend about which cryptoassets would be listed on the exchange (this usually led to a significant increase in its price). Wahi worked on the team that selected the cryptoassets to be listed on the exchange. In total, the fraudsters traded 55 cryptoassets using this scheme, raising $1.5 million. All three have already been convicted and, in addition to prison sentences, must also pay back everything they fraudulently obtained.[70] In addition, they entered into an agreement with the Securities and Exchange Commission that made certain of the cryptoassets traded a security. However, it is questionable whether the courts would have reached the same conclusion had the case come before them.[71]

---

67 Dimitris Kafteranis, Huseyin Unozkan, & Umut Turksen. (2023). COMPLIANCE AND ENFORCEMENT CHALLENGES IN TRADING OF NON-FUNGIBLE TOKENS. *International Journal of Law in a Changing World*, 2(3), 18-51. https://doi.org/10.54934/ijlcw.v2i3.57

68 *Former Employee Of NFT Marketplace Sentenced To Prison In First-Ever Digital Asset Insider Trading Scheme*. (2023, 22 August). Justice.gov; U.S. Attorney's Office, Southern District of New York. https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-sentenced-prison-first-ever-digital-asset-insider

69 Bose, P., Das, D., Gritti, F., Ruaro, N., Kruegel, C., & Vigna, G. (2023). Exploiting Unfair Advantages: Investigating Opportunistic Trading in the NFT Market. ArXiv (Cornell University). https://doi.org/10.48550/arxiv.2310.06844

70 Former Coinbase Insider Sentenced In First Ever Cryptocurrency Insider Trading Case. (2023, May 9). Justice.gov; U.S. Attorney's Office, Southern District of New York. https://www.justice.gov/usao-sdny/pr/former-coinbase-insider-sentenced-first-ever-cryptocurrency-insider-trading-case

71 *Former Coinbase Manager and His Brother Agree to Settle Insider Trading Charges Relating to Crypto Asset Securities*. (2023). Sec.gov. https://www.sec.gov/newsroom/press-releases/2023-98

The apparent tolerance of insider trading in the cryptocurrency market prior to 2023 can be attributed to several interconnected factors. The nascent nature of the cryptocurrency market and the absence of tailored regulations created an environment of regulatory ambiguity, leaving the legality of insider trading undefined. This ambiguity, coupled with the challenges of detection and prosecution in a decentralized and pseudonymous market, may have led to a perception that insider trading was not actively monitored or enforced. Furthermore, the rapid growth and volatility of the market may have overshadowed concerns about insider trading, while limited regulatory resources and a lack of public awareness further contributed to its perceived acceptance. The 2023 cases, therefore, may signify a turning point, reflecting a shift in legal interpretation and enforcement priorities as regulators recognize the need to address insider trading in this evolving market.

4.4 XIXOIO

The XIXOIO project is a Czech investment platform, founded in 2018, which focuses on the so-called tokenization of companies to enable companies to issue corporate tokens, a kind of digital equivalent of shares stored on the blockchain. Ownership of a corporate token is supposed to be associated with a share of the profits of the respective company. While the XIX token, belonging directly to XIXOIO, is the most prominent, several companies within the XIXOIO ecosystem have indeed issued their own corporate tokens. These tokens, however, are not traded on any mainstream cryptocurrency exchange and the secondary market for them is virtually non-existent. Despite many controversies, the purchase of the XIX token is still possible on the project's website, but its value is unilaterally set by the company itself. The project also included a commission system for bringing in new investors.[72]

The XIXOIO project became widely known through a massive advertising campaign in the autumn of 2021. However, critics of the XIXOIO project have pointed out from the beginning the risky nature of the investment and the unbalanced contractual terms, which do not provide investors with any certainty regarding the payment of profit shares or the redemption of XIX tokens.[73] Although the company, according to its own statements, was in contact with the Czech National Bank from the beginning, the latter refuted this information and at the same time warned against investing in unregulated corporate tokens that are not subject to legal investor protection.[74] A cautious warning, not specifically mentioning the XIXOIO project but apparently responding to its then ongoing advertising campaign, was also issued by the Ministry of Finance.[75]

72 XIXOIO a.s. *Product terms and conditions of token XIX of XIXOIO a.s.*, valid from 1 August 2021. https://media.graphassets.com/wH9xgS9GSTiBgk9To4c2

73 Úšela, J. (2021, December 10). *He has a cult in the company, but he doesn't understand technology, ormer employees say. We profile the head of the controversial Xixoio company*. Deník N. https://denikn.cz/764062/ve-firme-ma-kult-technologii-ale-nerozumi-rikaji-byvali-zamestnanci-prinasime-profil-sefa-kontroverzni-firmy-xixoio/

74 *Notice on the presentation of XIXOIO*. (2021). CNB.cz; Czech National Bank. https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/upozorneni/Upozorneni-k-prezentaci-spolecnosti-XIXOIO/.

75 *Treasury's Alert on the Risks of Investment Tokens* (2024). Ministry of Finance of the Czech Republic; Department of Financial Markets II. https://www.mfcr.cz/cs/financni-trh/bankovnictvi-a-dohled/platebni-sluzby-a-vyporadani-obchodu/aktuality/2021/upozorneni-ministerstva-financi-na-rizik-43725

In December 2023, Czech police filed criminal charges against Richard Watzke and Henry Ertner, the founders of the XIXOIO project, on suspicion of fraud under Section 209(1) and (5)(a) of the Criminal Code. The criminal prosecution itself commenced in November 2022, while the formal filing and subsequent reporting occurred later. The accused were alleged to have made false promises of savings appreciation through investments in the XIXOIO ecosystem, while deliberately providing misleading information to investors. The funds extorted from the 2,931 victims exceeded CZK 339 million (USD 14.6 million) and EUR 571,000 (USD 624,635.43), and were allegedly used to operate the company, pay commissions, purchase real estate, or pay for the expensive living expenses of the project's founders.[76] According to available information, the prosecution has not yet been completed at the time this article was submitted.

4.5 Case Studies: A Comparative Perspective

The case studies presented above serve a multifaceted purpose within the broader comparative analysis of cryptocurrency regulation and enforcement in the United States and the Czech Republic.

Firstly, the cases function as illustrative exemplars, offering concrete examples of the diverse and evolving nature of fraudulent schemes prevalent in the cryptocurrency market. They underscore the potential for investor harm and the need for robust regulatory frameworks to mitigate such risks.

Secondly, the inclusion of cases from both jurisdictions facilitates a comparative analysis of regulatory responses and enforcement approaches. By examining the outcomes of these cases, the article assesses the effectiveness of each system in deterring fraudulent activities, prosecuting perpetrators, and recovering investor funds.

Thirdly, the case studies provide empirical evidence to inform recommendations for enhancing the Czech regulatory framework. Drawing on lessons learned from the US experience, the article suggests specific measures to improve and strengthen enforcement capabilities in the Czech Republic.

Evaluation of Cases and Regulatory Systems:

- OneCoin and BitConnect: These cases illustrate the transnational nature of cryptocurrency fraud and the associated jurisdictional challenges. The US response, characterized by multi-agency collaboration and the adaptation of existing laws, demonstrates both the strengths and potential complexities of their approach.
- Insider Trading Cases (Nathaniel Chastain and Ishan Wahi): These cases highlight the adaptability of US securities laws to address novel forms of insider trading in the cryptocurrency market. They underscore the importance of proactive enforcement and the potential for leveraging blockchain technology to detect and prosecute illicit activities.
- XIXOIO: This case exposes the limitations of the current Czech regulatory framework, which is characterized by a reactive approach and a lack of specialized tools for addressing

76 Ibehei, J. (2023b). *Indictment of persons in connection with the XIXOIO case*. Policie.cz. https://www.policie.cz/clanek/obvineni-osob-v-souvislosti-s-pripadem-xixoio.aspx

cryptocurrency-specific fraud. It emphasizes the need for greater regulatory clarity, proactive enforcement, and public awareness campaigns to protect investors in the Czech Republic.

The case studies also delineate the crucial distinction between outright scams, such as OneCoin and XIXOIO, and regulatory investigations arising from legal ambiguities surrounding the application of existing laws to novel cryptocurrency products and practices. This distinction underscores the importance of developing clear and comprehensive regulations in the Czech Republic to provide legal certainty and reduce the potential for exploitation due to regulatory gaps.

In summary, the case studies serve as integral components of the comparative analysis, providing empirical evidence, illustrating key concepts, and informing recommendations for regulatory improvements. They contribute to a deeper understanding of the challenges and opportunities in regulating the cryptocurrency market, ultimately aiming to enhance enforcement and foster a more secure and transparent cryptocurrency ecosystem.

5. Comparative analysis of the US and Czech approaches to cryptocurrency fraud

The approaches of the United States and the Czech Republic to regulating cryptocurrency fraud differ significantly, and each has its own strengths and weaknesses. The United States boasts a robust legal framework, which has been adapted to the rapid rise in popularity of cryptoassets through flexible interpretation of existing securities and commodities laws. For example, the US Securities and Exchange Commission (SEC) applies the Howey test to cryptoassets, which has traditionally been used to determine whether a financial asset constitutes a security. This proactive legal interpretation allows the US to regulate and protect investors without having specialized legislation at the beginning of the crypto boom. In addition to this legislative adaptability, US authorities, including the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and the Department of Justice (DOJ), have worked extensively together to monitor various aspects of the cryptocurrency market. Their efforts are supported by the use of advanced technological tools, such as blockchain analytics and other data-driven investigative techniques, to help detect fraudulent activity and trace cryptoassets from illegal activity. In addition, U.S. authorities assert jurisdiction over international cases where fraud affects U.S. citizens even when the fraudulent activity occurs outside the U.S., allowing for global reach of their enforcement efforts. The manner in which U.S. regulators seek to warn the public about the risks of fraud in the cryptoasset market or to economically incentivize potential whistleblowers is also inspiring.[77]

However, the US approach is not without problems. The involvement of multiple regulators, each with overlapping jurisdiction, can create confusion among market participants and also

77 Eakeley, D., Guseva, Y., Choi, L., & Gonzalez, K. *CRYPTO-ENFORCEMENT AROUND THE WORLD*. Retrieved October 12, 2024, from https://southerncalifornialawreview.com/wp-content/uploads/2021/05/Eakeley-and-Guseva_Final-2021.pdf

lead to gaps in enforcement. Legitimate businesses may also be deterred from entering the market. Moreover, while existing laws have been adapted to address crypto-related fraud, they were designed for traditional financial instruments and are not always tailored to address the unique characteristics of crypto-assets, leaving room for improvement in the legal framework.

Czech legislation, on the other hand, does not yet offer a specialised, but not very adaptable legal framework comparable to that of the United States, although this can be expected to improve substantially with the upcoming implementation of MiCA. Nevertheless, the Czech authorities have in several cases been able to address cryptocurrency fraud by prosecuting offenders under traditional legal offences such as theft, embezzlement and fraud. This approach, although not specifically tailored to cryptoassets, has provided a degree of legal protection. In addition, the Czech authorities have demonstrated competence in seizing and monetising crypto-assets, which is an extremely important element in the fight against digital crime, as the crime must not be economically rewarding.

Despite these enforcement efforts, the Czech regulatory framework for cryptoassets remains underdeveloped. The lack of clear legal definitions of cryptoassets and their classification as securities, commodities or other financial instruments, and the involvement of traditional authorities such as the CNB, the Ministry of Finance and the Financial Analysis Office, hinder the creation of a safe environment. In addition, public authorities can be criticised for being slow to react to suspicious investment opportunities, as illustrated by the XIXOIO case, where state intervention came more than two years apart, unnecessarily leading to significant investor losses. Although experts pointed out suspicious aspects of the project from the beginning, the relevant state authorities (Ministry of Finance, Czech National Bank) limited themselves to warnings and declarations that the matter did not fall within their competence. The criminal prosecution against the founders of the project in November 2024 is ongoing and the XIX token can still be purchased on the project's website. This approach contrasts with the more proactive stance of US regulators, who often act in a timely manner to prevent escalation.

Another area where the Czech authorities could draw inspiration is the use of modern technological tools. Unlike their US counterparts, Czech law enforcement agencies have not adopted blockchain analytics and other data-driven methods to detect fraud, which creates room for fraudulent activities to go undetected for longer. The introduction of advanced investigative methods would enable Czech authorities to detect and investigate cryptocurrency fraud more effectively.

While Czech law enforcement agencies have been somewhat slower to adopt blockchain analytics and other data-driven methods compared to their US counterparts, it's important to acknowledge that these tools are not entirely absent from their investigative arsenal. The Czech police have, in fact, utilized blockchain analysis in certain high-profile cases, demonstrating a growing awareness of their potential value in combating cryptocurrency-related crime. However, the use of these technologies remains limited due to factors such as resource constraints, technical expertise gaps, and a historical reliance on traditional investigative techniques. As the cryptocurrency market continues to evolve and the sophistication of cybercrime increases, wider adoption of blockchain analytics and other data-driven methods will be crucial for Czech law enforcement agencies to effectively detect, investigate,

and prosecute cryptocurrency fraud. However, the Czech public authorities should take a more proactive stance in dealing with suspicious investment projects and act in a timely manner to mitigate potential damage to investors. Finally, greater international cooperation and the exercise of jurisdiction even in the case of cross-border fraud would also strengthen Czech efforts to combat cryptocurrency fraud.

While it could be argued that the Czech Republic does not need such a robust regulatory framework, as it is a much smaller market compared to the US, it is clear from practice that fraudsters are targeting Czech investors. In summary, therefore, while the US excels at proactive and coordinated enforcement, backed by advanced technology and international reach, the Czech Republic has the potential to strengthen its regulatory and enforcement capabilities as it moves towards a more comprehensive legal framework for cryptocurrencies. If the Czech Republic draws inspiration from the strengths of the U.S. approach, it can more effectively combat cryptoassets frauds.

6. Conclusion

Both the US and Czech legal environments have strengths and weaknesses in combating cryptocurrency fraud. The U.S. benefits from a proactive and flexible regulatory approach with strong enforcement capabilities that are enhanced by advanced technology and international cooperation. In contrast, the Czech Republic is still developing a specialised legal framework, although it has demonstrated competence in the seizure and monetisation of crypto-assets derived from criminal activity. However, slower responses to clear cases of fraud point to the need for a more proactive approach. However, with the transposition of the MiCA Regulation, improvements in the Czech legal environment can be expected to provide a more comprehensive framework for dealing with these cases. Nonetheless, drawing lessons from the U.S. approach could further enhance enforcement in the Czech Republic.

List of literature

1. Academic Resources

Allen, B., Brez, Z., Kalil, C., Kasulis, J., & Mouritsen, S. (2024). *DOJ and SEC crypto exchange enforcement in the United States*. Globalinvestigationsreview.com. https://globalinvestigationsreview.com/review/the-investigations-review-of-the-americas/2025/article/doj-and-sec-crypto-exchange-enforcement-in-the-united-states

Andhov, A. (2021). Wyoming's Wild West Blockchain Laws and a Start-up Lobby. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3898451

Baker, B. (2017). Application of the New York BitLicense to Initial Coin Offerings. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3319540

Bartlett, J. (2023). *The Missing Cryptoqueen*. Ebury Publishing.

Bose, P., Das, D., Gritti, F., Ruaro, N., Kruegel, C., & Vigna, G. (2023). Exploiting Unfair Advantages: Investigating Opportunistic Trading in the NFT Market. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2310.06844

Chohan, U. (2018). Bitconnect and Cryptocurrency Accountability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3131512

Dimitris Kafteranis, Huseyin Unozkan, & Umut Turksen. (2023). COMPLIANCE AND ENFORCEMENT CHALLENGES IN TRADING OF NON-FUNGIBLE TOKENS. *International Journal of Law in a Changing World*, *2*(3), 18-51. https://doi.org/10.54934/ijlcw.v2i3.57

Eakeley, D., Guseva, Y., Choi, L., & Gonzalez, K. (n.d.). *CRYPTO-ENFORCEMENT AROUND THE WORLD*. Retrieved October 12, 2024, from https://southerncalifornialawreview.com/wp-content/uploads/2021/05/Eakeley-and-Guseva_Final-2021.pdf

Fischer, J. (2024). *Reflection of cryptocurrencies in selected areas of criminal law* [Master's thesis (Mgr.)]. https://theses.cz/id/7tpslf/

Innocent Chiluwa. (2019). "Truth," Lies, and Deception in Ponzi and Pyramid Schemes. *IGI Global EBooks*, 439-458. https://doi.org/10.4018/978-1-5225-8535-0.ch023

Kshetri, N. (2022). Scams, Frauds, and Crimes in the Nonfungible Token Market. *Computer*, *55*(4), 60-64. https://doi.org/10.1109/MC.2022.3144763

Nolasco Braaten, C., & Vaughn, M. S. (2019). Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions. *Deviant Behavior*, *42*(8), 1-21. https://doi.org/10.1080/01639625.2019.1706706

Plecitý, D. (n.d.). AML REGULATION: Cryptocurrencies and laundering of proceeds of crime. *Bankingonline.cz*. Retrieved October 19, 2024, from https://fau.gov.cz/files/kryptomeny-a-legalizace-vynosu-z-trestne-cinnosti.pdf

Saha, S., Ahmed Rizvan Hasan, Mahmud, A., Ahmed, N., Parvin, N., & Hemal Karmakar.(2024). Cryptocurrency and financial crimes: A bibliometric analysis and future research agenda. *Multidisciplinary Reviews*, *7*(8), 2024168-2024168. https://doi.org/10.31893/multirev.2024168

SEC Declares Bitcoin and Ether as Non-Securities. (n.d.). Cassels. https://cassels.com/insights/sec-declares-bitcoin-and-ether-as-non-securities/

Spilka, D. (2023, May 16). *What does the adoption of cryptocurrencies in the Czech Republic mean from a legal perspective?* Legal Space. https://www.pravniprostor.cz/clanky/financni-pravo/co-znamena-prijeti-kryptomen-v-ceske-republice-z-pravniho-hlediska.

Susan Low Bloch, & Jackson, V. *Federalism: a reference guide to the United States Constitution*. Praeger, An Imprint Of Abc-Clio, Llc.

Tan, C. (2024). Rights in NFTS and the flourishing of NFT marketplaces. *International Journal of Law and Information Technology*, *32*(1). https://doi.org/10.1093/ijlit/eaae018

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1). https://doi.org/10.1186/s40163-021-00163-8

Zhang, A. R., Raveenthiran, A., Mukai, J., Naeem, R., Dhuna, A., Parveen, Z., & Kim, H. (2019). The Regulation Paradox of Initial Coin Offerings: A Case Study Approach. *Frontiers in Blockchain*, *2*. https://doi.org/10.3389/fbloc.2019.00002

2. Newspaper articles

Bing, C. (2021, June 7). *U.S. seizes $2.3 million in bitcoin paid to Colonial Pipeline hackers*. Reuters. https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/.

CTK. (2019, September 5). *Court reconsiders bitcoin theft to embezzlement, programmer gets 9 years - iDNES.cz*. IDNES.cz. https://www.idnes.cz/brno/zpravy/soud-programator-tomas-jirikovsky-bitcoiny-zpronevera.A190905_121842_brno-zpravy_krut

Davis, D., & Kim, A. (2024, July 9). *Ether's Legal Status Clarified? CFTC Scores Win as Court Backs Agency's Commodity Classification*. Katten. https://quickreads.ext.katten.com/post/102jcc8/ethers-legal-status-clarified-cftc-scores-win-as-court-backs-agencys-commodity#page=1

Kateřina Vaníčková. (2024, May 4). *State sends over 4 bitcoins to auction, starting price exceeds CZK 6 million - iDNES.cz*. IDNES.cz. https://www.idnes.cz/zpravy/domaci/stat-majetek-prodej-virtualni-mena-miliony-korun-bitcoin-aukce.A240504_103127_domaci_vank

O'Melveny & Myers LLP. (2024, October 18). *The Ever-Shifting Landscape of U.S. Crypto Regulation*. OMM.com. https://www.omm.com/insights/alerts-publications/the-ever-shifting-landscape-of-us-crypto-regulation/

Penman, A. (2016, February 10). *Here's why hyped-up web currency OneCoin is virtually worthless*. The Mirror. https://www.mirror.co.uk/news/uk-news/who-wants-onecoin-millionaire-you-7346558

Úšela, J. (2021, December 10). *He has a cult in the company, but he doesn't understand technology, former employees say. We profile the head of the controversial Xixoio company*. Deník N. https://denikn.cz/764062/ve-firme-ma-kult-technologii-ale-nerozumi-rikaji-byvali-zamestnanci-prinasime-profil-sefa-kontroverzni-firmy-xixoio/

Yang, Y. (2018, May 29). *China prosecutes 98 people, recovers US$268 million in OneCoin cryptocurrency investigation, report says*. SCMP.com; South China Morning Post. https://www.scmp.com/tech/article/2148114/china-prosecutes-98-people-recovers-us268-million-onecoin-cryptocurrency

3. Press releases

$4 Billion Crypto-Promoter Ordered to Halt Fraudulent Sales. (2022). Texas.gov; Texas State Securities Board. https://ssb.texas.gov/news-publications/4-billion-crypto-promoter-ordered-halt-fraudulent-sales

5 Ways Fraudsters May Lure Victims Into Scams Involving Crypto Asset Securities - Investor Alert. (2024). Investor.gov; U.S. Securities and Exchange Commission. https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/crypto-scams

CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange | CFTC. (n.d.). Www.cftc.gov. https://www.cftc.gov/PressRoom/PressReleases/8680-23

Co-Founder Of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced To 20 Years In Prison. (2023, September 12). Justice.gov; U.S. Attorney's Office, Southern District of New York . https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison

Crypto Fraud Victims Receive Over $17 Million in Restitution from BitConnect Scheme. (2023, Jan. 12). Justice.gov; Office of Public Affairs. https://www.justice.gov/opa/pr/crypto-fraud-victims-receive-over-17-million-restitution-bitconnect-scheme

Emergency Cease and Desist Order (BitConnect), (Texas State Securities Board, Jan. 4, 2018). https://www.ssb.texas.gov/sites/default/files/BitConnect_ENF-18-CDO-1754.pdf

Former Coinbase Insider Sentenced In First Ever Cryptocurrency Insider Trading Case. (2023, May 9). Justice.gov; U.S. Attorney's Office, Southern District of New York. https://www.justice.gov/usao-sdny/pr/former-coinbase-insider-sentenced-first-ever-cryptocurrency-insider-trading-case

Former Coinbase Manager and His Brother Agree to Settle Insider Trading Charges Relating to Crypto Asset Securities. (2023). Sec.gov. https://www.sec.gov/newsroom/press-releases/2023-98

Former Employee Of NFT Marketplace Sentenced To Prison In First-Ever Digital Asset Insider Trading Scheme. (2023, 22 August). Justice.gov; U.S. Attorney's Office, Southern District of New York. https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-sentenced-prison-first-ever-digital-asset-insider

Former Law Firm Partner Sentenced To 10 Years In Prison For Laundering $400 Million Of OneCoin Fraud Proceeds. (2024, January 25). Justice.gov; U.S. Attorney's Office, Southern District of New York . https://www.justice.gov/usao-sdny/pr/former-law-firm-partner-sentenced-10-years-prison-laundering-400-million-onecoin-fraud

Ibehej, J. (2023a). *Investment fraud worth more than CZK 1 billion - Police of the Czech Republic*. Policie.cz. https://www.policie.cz/clanek/investicni-podvod-za-vice-nez-1-miliardu-korun.aspx

Ibehei, J. (2023b). *Charges against persons in connection with the XIXOIO case - Police of the Czech Republic*. Policie.cz. https://www.policie.cz/clanek/obvineni-osob-v-souvislosti-s-pripadem-xixoio.aspx

On the possibility for investment funds to invest in cryptoassets. (2021). Czech National Bank. https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/stanoviska-k-regulaci-financniho-trhu/RS2023-05/.

Media Communication Department. (2024). *The government approved the Digital Finance Act | Ministry of Finance*. Ministry of Finance. https://www.mfcr.cz/cs/ministerstvo/media/tiskove-zpravy/2024/vlada-schvalila-zakon-o-digitalnich-financich-55549

NOTICE - OneCoin - Financial Supervision Commission. (2015, September 30). Financial Supervision Commission. https://www.fsc.bg/saobshtenie-onecoin/

SEC.gov | BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product. (n.d.). Www.sec.gov. https://www.sec.gov/newsroom/press-releases/2022-26

SEC.gov | SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering. (2020). Sec.gov. https://www.sec.gov/newsroom/press-releases/2020-338

Up to $5 Million Reward Offer for Information Leading to Arrest and/or Conviction of Cryptocurrency Fraudster Ruja Ignatova - United States Department of State. (2024). United States Department of State. https://www.state.gov/up-to-5-million-reward-offer-for-information-leading-to-arrest-and-or-conviction-of-cryptocurrency-fraudster-ruja-ignatova/

Notice on the presentation of XIXOIO. (2021). CNB.cz; Czech National Bank. https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/upozorneni/Upozorneni-k-prezentaci-spolecnosti-XIXOIO/.

Ministry of Finance warning on the risks of investment tokens | Ministry of Finance of the Czech Republic (2024). Ministry of Finance of the Czech Republic; Department of Financial Markets II. https://www.mfcr.cz/cs/financni-trh/bankovnictvi-a-dohled/platebni-sluzby-a-vyporadani-obchodu/aktuality/2021/upozorneni-ministerstva-financi-na-rizik-43725

4. Legislation

Commodity Exchange Act of 1936, 7 U.S.C. § 1 et seq. (1936).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience in the financial sector

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets for cryptoassets

Chamber of Deputies of the Parliament of the Czech Republic (2024, 3 May). *Draft Act on the Digitization of the Financial Market*. Chamber of Deputies Print 692. https://www.psp.cz/sqw/historie.sqw?o=9&T=692.

Securities Act of 1933, 15 U.S.C. § 77a et seq. (1933).

Securities Exchange Act of 1934, 15 U.S.C. § 78a et seq. (1934).

U.S. Constitution

Act No. 253/2008 Coll., on Certain Measures against the Legalization of the Proceeds of Crime and the Financing of Terrorism, as amended

Act No. 256/2004 Coll., on Capital Market Business, as amended.

Act No. 40/2009 Coll., Criminal Code, as amended

Act No. 455/1991 Coll., on Trade Enterprise (Trade Licensing Act), as amended.

Act No. 89/2012 Coll., Civil Code, as amended.

5. Court decisions and legal actions

Complaint against BitConnect, Satish Kumbhani, Glenn Arcaro, and Future Money Ltd, (U.S. Securities and Exchange Commission, September 1, 2021). https://www.sec.gov/files/litigation/complaints/2021/comp-pr2021-172.pdf

U.S. Supreme Court (n.d.). *SEC v. Howey Co., 328 U.S. 293 (1946)*. Justia Law. https://supreme.justia.com/cases/federal/us/328/293/

6. Website

Criminal Division | Crypto Enforcement. (2022, July 5). Www.justice.gov. https://www.justice.gov/criminal/criminal-fraud/crypto-enforcement

Crypto Assets. (n.d.-a). Sec.gov; U.S. Securities and Exchange Commission. https://www.sec.gov/securities-topics/crypto-assets

Crypto Assets. (n.d.-b). Investor.gov; U.S. Securities and Exchange Commission. https://www.investor.gov/additional-resources/spotlight/crypto-assets

SEC.gov | Office of Strategic Hub for Innovation and Financial Technology (FinHub). (2023). Sec.gov. https://www.sec.gov/about/divisions-offices/office-strategic-hub-innovation-financial-technology-finhub

SEC.gov | Whistleblower Program. (n.d.). Www.sec.gov. https://www.sec.gov/enforcement-litigation/whistleblower-program

7. Other sources

XIXOIO a.s. *Product terms and conditions of token XIX of XIXOIO a.s.*, valid from 1 August 2021. https://media.graphassets.com/wH9xgS9GSTiBgk9To4c2

Mgr. Tomáš Brandejský is a PhD candidate in his third year at the Prague University of Economics and Business, specializing in financial law and regulation. His research focuses on the legal aspects of cryptocurrency markets, with a particular interest in the prevention of fraud involving cryptoassets and NFTs. As part of the IGS grant project "Prevention of Crypto Asset Fraud and Failure of Related Service Providers in an International Context", he explores regulatory responses to emerging financial technologies, comparing enforcement practices in the US and the Czech Republic.