DOI: 10.38146/BSZ-AJIA.2025.v73.i11.pp2361-2372

Invisible money, visible crime? The emergence of cryptocurrencies in economic crime

Bálint Gábor Nagy
Dr., Prosecutor General, Adjunct Lecturer
The Prosecution Service of Hungary,
Pázmány Péter Catholic University,
Faculty of Law and Political Science
lu@mku.hu

Abstract

Aim: The aim of this study is to explore the relationship between economic crime and cryptocurrencies, particularly with regard to the role that crypto assets can play in the commission of economic crimes and in removing illicitly obtained assets from the authorities' purview. The main hypothesis is that cryptocurrencies can be interpreted not only as a financial innovation, but also as a means of opening up new dimensions in the field of crime.

Methodology: The analysis is based on qualitative research methods, drawing on the law enforcement experience of the prosecution office and the findings of a targeted investigation conducted by the Prosecutor General's Office into cryptocurrencies.

Findings: The primary finding of the study is that the decentralized, pseudo-anonymous nature of cryptocurrencies can pose significant risks: it can facilitate the spread of economic crime and also affect the structure of economic crimes. The anonymity and easy access characteristic of cryptocurrencies hinder the effective action of law enforcement authorities in detecting and prosecuting perpetrators. Crypto assets are also suitable for withdrawing criminal proceeds from the authorities.

Value: The study highlights that, thanks to technological advances and the spread of digitalization, economic criminals now have a wider range of tools at their disposal. White-collar criminals have no particular problem adapting

English-language republication. The Hungarian version of this article was published in Belügyi Szemle 2025, issue 11. DOI link: https://doi.org/10.38146/BSZ-AJIA.2025.v73.i11.pp2209-2222

to the changed global circumstances; in fact, they use them to their advantage when committing crimes. The prosecution's experience in applying the law and its investigation into cryptocurrencies can contribute to the development of law enforcement practices.

Keywords: economic crime, cryptocurrencies, digitalization, prosecution

Introduction – Actual trends in economic crime

Economic crime is one of the most complex forms of crime today, causing not only financial damage but also distorting the functioning of the economy and, in the long term, undermining confidence in the rule of law. A fundamental characteristic of economic crime is that it poses a threat not only to the economy of a given nation, but also to the economic and financial system globally. With regard to these crimes – as with other punishable behaviors – it can be said that, in terms of total crime, there is a tendency for cross-border offenses involving several countries to be quite common, as it is no longer particularly difficult for criminals to cross national borders quickly and with as few traces as possible. Crossing national borders can be done not only physically but also digitally, which facilitates the commission of crimes and can also increase their effectiveness.

The growing international nature of economic crime has therefore been aided by global phenomena that transcend crime, such as the spread of digitalization and the blurring of national borders.

It is important to note that, partly due to their international nature and partly due to the complexity of their commission, economic crimes in most cases require the organized participation of multiple perpetrators. For this reason, organized and economic crime are often intertwined, each posing a serious social and economic threat on its own, and together presenting unprecedented challenges for both legislation and law enforcement.

The assessment of economic crimes is further complicated by the fact that the conduct constituting these crimes can be extremely diversified and is often linked to other types of crimes, such as corruption, crimes against public trust, or even crimes against property. With regard to the effectiveness of law enforcement, it should be noted that in criminal proceedings for economic crimes, it is not enough for investigators, prosecutors, and judges to have a thorough knowledge of criminal law; they also need to have expertise in economics or even accounting.

Another important consideration is that digitization–along with the blurring of national borders–makes it easier for perpetrators to remain anonymous in the online space and to conceal illicitly obtained wealth.

Parallel to the continuous expansion of the digital space, the toolkit of economic crime has also broadened. It is particularly worrying that, contrary to their original purpose, the new financial instruments created by technological developments have become increasingly suitable for concealing economic crimes and laundering illicitly obtained assets. One of the most striking examples of this is the emergence and rapid spread of cryptocurrencies. Cryptocurrencies are increasingly associated with money laundering and economic crimes, and provide financial backing for organized crime, which is why these dual-purpose financial instruments deserve special attention from a criminal law perspective.

The experiences of law enforcement officials in budget fraud cases from the perspective of the public prosecutor's office

Within the scope of economic crimes, budget fraud is considered a typical offense that has a particularly sensitive impact on the state budget and the balance of public finances. For this reason, the procurator general usually provides a specific overview of the current trends in budget fraud in his report to the parliamentary report.

Looking at the statistics for 2023, there was a slight decrease in the number of registered crimes related to budget fraud. However, this decrease did not automatically mean that the workload of the public prosecutor's office related to criminal proceedings initiated for crimes affecting the budget would also decrease. One reason for this is that criminal proceedings initiated complex budget fraud affecting several Member States and typically carried out by criminal organizations, which are becoming more common.

In these criminal cases, it is not uncommon for the amount of financial loss to reach hundreds of millions or even billions. The complexity of such cases is also evident in the process of proving them, which usually requires a variety of time-consuming procedural steps and the simultaneous use of various forms of legal assistance, both during the investigation and the examination phase. It should be noted that the new special procedure included in Act XC of 2017 on Criminal Procedure (hereinafter: Be.) and applicable from January 2023, the so-called supplementary private prosecution procedure, shall also be applied in cases of budget fraud, provided that the conditions are met, as the legislator has specifically mentioned crimes causing damage to the budget among the priority crimes related to the exercise of public authority or the management of

public assets. The experience of prosecutors in 2023 showed that even in the year when the new legal institution was introduced, a significant proportion of priority crimes were crimes damaging the budget.

As regards the methods used to commit budget fraud, the experience of the public prosecutor's office shows that the methods used on the revenue side appear to be becoming more constant. Thus, the use of subcontractors, or so-called 'front companies,' continues to be a frequently observed technique in organized crime. This method of committing crimes is particularly popular in the area of services requiring large human resources, with companies operating primarily in the areas of property protection and cleaning using it to avoid paying contributions for their employees. Meanwhile, they reduce their VAT liability based on false invoices issued by 'shell companies.' An improved version of this now 'traditional' method has also appeared, whereby perpetrators disguise employment as temporary staffing and, in order to avoid detection, register some of the employees with the tax authorities.

Another form of crime affecting the revenue side is VAT fraud, typically involving carousel fraud or the use of 'missing traders,' but simple tax evasion and classic methods of invoice fraud have also been the basis for several criminal cases. In comparison, less frequently detected types of crimes include 'company graveyard services,' where perpetrators purchase loss-making companies burdened with tax debts from each other, thereby shielding assets from tax enforcement.

Moving on to the expenditure side of budget fraud, one of the most typical forms of fraud is the overpricing of subsidized investments, a method by which perpetrators initiate the disbursement of subsidies in amounts higher than those legally claimable. In these criminal cases, false invoices are issued in order to account for unjustifiably high costs.

In criminal proceedings initiated for crimes that damage the budget or violate the rules of economic management, the primary objective of the public prosecutor's office is to repair the financial and property damage caused. This is achieved, on the one hand, by applying coercive measures restricting property rights and confiscating property for the benefit of the state and, on the other hand, by applying measures based on voluntary compliance by the perpetrator, primarily the obligation to pay compensation as stipulated in the settlement agreement. However, in the absence of cooperation, it is difficult to remedy financial and property rights violations if the proceeds of crime are laundered using cryptocurrencies. There are already examples of this, and we can reasonably expect the use of cryptocurrencies to increase in the future.[1]

1 B/8995. Report of the Procurator General to the National Assembly on the activities of the Prosecutor's Office in 2023 (pp. 22-27). (URL1).

The emergence and spread of cryptocurrency as an (illegal) financial instrument

Cryptocurrencies have become really widespread in recent years, with Bitcoin being the first and most widely known of them. Nowadays, however, the popularity of alternative cryptocurrencies, known as Altcoins, is also growing significantly. Crypto assets are also becoming increasingly accessible through cryptocurrency exchanges, and their trading volume has grown significantly in recent years despite high market volatility. Their potential uses have also expanded with the introduction of new asset types: non-monetary digital tokens (i.e. NFTs) can represent significant value as unique works of art [2], but in some cases they are created solely for money laundering purposes. The use of decentralized payment systems (known as DeFi) is also growing; these essentially provide a range of traditional financial services, but only in relation to crypto assets (Eurojust & EJCN, 2025). Parallel to the widespread acceptance of crypto assets, certain crimes have undergone a transformation and new offenses have emerged. Crimes related to cryptocurrencies can basically be divided into two groups: in the first case, cryptocurrency is the object of the crime, while in the second case, it is used to store the proceeds of crime (Polt, 2021).

In recent years, EU legislative processes related to cryptocurrencies have focused on transaction traceability and the prevention of money laundering and terrorist financing. In this context, the spread of blockchain-based payment instruments has made it urgent to create an EU legal instrument governing the market for crypto-assets. The European Parliament and Council Regulation (EU) 2023/1114 on markets in crypto assets (hereinafter: MiCA Regulation), which entered into force on December 30, 2024, is a milestone in comprehensive EU regulation. The fundamental objective of the MiCA Regulation was to establish uniform rules for issuers and service providers of crypto assets that are not yet regulated (URL2).

For the purposes of EU law, the concept of virtual currency is defined in Directive (EU) 2018/843 of the European Parliament and of the Council as follows: *'a digital representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily attached to regular money, and does not have the legal status of regular money or money, but is accepted by natural or legal persons as a means of exchange, and can be transferred, stored, and*

2 NFTs are non-fungible tokens that can also represent works of art. For example, a montage made from photos uploaded to social media was sold at an online auction for $69.3 million in cryptocurrency (Mezei, 2022).

traded electronically.'[3] Based on this directive, Act LIII. of 2017 on the prevention and combating of money laundering and terrorist financing (hereinafter: Pmt.) also defines the concept of virtual currency.[4] One of the most common characteristics of cryptocurrencies, and also the most striking difference compared to 'traditional' financial instruments, is that their issuance is not handled by a central authority or central bank, while their operation is based on blockchain technology and a decentralized peer-to-peer network. One of the main features of blockchain is that it ensures anonymity, which can be extremely attractive for illegal use (Eurojust & EJCN, 2025). Cryptocurrencies therefore enable a pseudo-anonymous and relatively fast way of moving funds globally, as well as being easy to buy and sell on various platforms. In terms of pseudo-anonymity, users are not completely anonymous, but they cannot be directly identified, as the address of a cryptocurrency wallet appears during transactions. However, it is important to note that although it is not possible to directly identify who is behind a transaction, it is possible to see between which addresses the money moved, and every transaction is public and traceable on the blockchain. The dual nature of cryptocurrencies means that in recent years they have become an investment solution, a payment solution, and the basis for various new financial constructs, but at the same time they are increasingly being used, for example, in darknet financial transactions, money laundering, and terrorist financing (Polt, 2021).

The use of cryptocurrencies by criminals is also becoming more common because the barriers to entry are low: users only need a device with an internet connection, and the mechanisms and processes are easy to learn without in-depth IT knowledge. Thanks to all these characteristics, the use of cryptocurrencies has become noticeable in recent years across a wider spectrum of crimes, including economic crimes. No data is available on the proportion of crypto asset transactions carried out for illegal purposes compared to all transactions. However, it is clear from criminal cases that perpetrators of wealth-generating crimes are converting assets acquired in traditional fiat currencies into crypto assets in increasing numbers and volumes, the amount of wealth acquired by criminals in cryptocurrency is growing, and virtual currencies, crypto exchanges, crypto brokers, and mixer service providers are now the primary supporters of money launderers' activities.

3 Article 1(2)(d) of Directive (EU) 2018/843 of the European Parliament and of the Council.

4 According to Section 3(47) of the Pmt., virtual currency is: 'a digital representation of value that is not issued or guaranteed by a central bank or public authority; does not have the legal status of legal tender; can be stored electronically, is accepted as a medium of exchange, and is therefore particularly suitable for electronic transfer and electronic trading.'

Key findings of the prosecutor's investigation into cryptocurrencies

In 2021, the Prosecutor General's Office conducted a targeted investigation into the practice of seizing and freezing electronic money and virtual payment instruments. The investigation looked at the types of criminal cases in which electronic money or cryptocurrency was seized or frozen, and whether these coercive measures were ordered and executed in accordance with the law. An important part of the investigation was also to assess what measures, if any, the investigating authority takes to trace electronically existing or virtual assets when searching for assets derived from crime.

There is no data available on the proportion and value of transactions involving the use of cryptocurrencies for criminal purposes that violate economic order and damage the budget, or money laundering. However, as a result of the targeted investigation, a total of seven criminal cases were identified in which cryptocurrencies were seized. Of these seven cases, two were for budget fraud, two for drug trafficking, one for money laundering, one for fraud, and one for theft. In both criminal cases involving budget fraud, the cryptocurrency in the virtual wallet was seized and transferred to virtual wallet addresses managed by the investigating authority. In all cases, the investigating authority ensured the seizure of the cryptocurrency by performing an operation that prevented the disposal of the cryptocurrency and the use of the electronic data used for payment. The legal basis for the seizure was, in all cases, to ensure the confiscation of assets.

Among other things, the investigation also examined whether the Criminal Code and other provisions provide an adequate legal framework. With regard to the Criminal Code, the legislator has set as a priority the more effective confiscation of assets derived from criminal activity. For this reason, the Criminal Code imposes an obligation on both the public prosecutor's office and the investigating authority to take all necessary measures during criminal proceedings to identify and secure items or assets that are subject to confiscation or asset forfeiture.[5] In line with developments in cash flow, the Be. also created an explicit legal possibility for the seizure of assets existing in electronic or virtual form by including electronic money among the possible objects of seizure and introducing supplementary regulations concerning electronic data used for payment in the area of electronic data.[6]

5 Be. Section 353(1).
6 Be. Section 308(3), Section 311(1)(d) and Section 315(2).

The investigation clearly concluded that the legal framework is adequate, even though the regulations do not cover every detail. Problems and questions that arise and are not covered by the legislation have been answered in practice, and these cases are also addressed in the individual organizations' own cryptocurrency seizure guidelines. Such guidelines have been developed by the Cybercrime Department of the National Bureau of Rapid Response and Special Police Service, then in 2022-2023 the National Tax and Customs Administration, in cooperation with the police, the Prosecutor General's Office, and the Ministry of Justice in 2022-2023 developed another one, which was issued in the form of a circular letter from the President of the NAV.

Based on the findings of the investigation, the Prosecutor General's Office identified a general and systemic problem in the recovery of criminal assets, namely that in proceedings relating to asset-generating crimes, the investigating authorities – with very few exceptions – only took action to trace virtual assets if there was evidence of their use or possession. In only 1.1% of the cases investigated for asset-generating crimes (630 cases) were cryptocurrencies seized. Even considering the fact that in some of the cases there was no realistic chance that the perpetrators or other persons would have virtual assets that could be confiscated, this was an extremely low proportion. It was therefore necessary to change this investigative practice. The Prosecutor General's Office assigned the following task to lower-level prosecutor's offices: when conducting investigations, they should require the investigating authorities to go beyond requesting data from official records and credit institutions in investigations into wealth-generating crimes, and to search for cryptocurrency exchanges and wallet providers in Hungary and conduct searches at the places of residence or stay of the suspects.

In order to locate assets subject to confiscation, to be returned to the injured party, or to satisfy civil law claims, investigating authorities had to start taking active measures not only when they had info pointing to the possible existence of such assets, but also in all cases where the possession of electronic money/virtual currency could reasonably be assumed, or at least could not be ruled out. To substantiate this assumption, investigating authorities must assess the specific characteristics of the crime and the personal circumstances of the perpetrator, as well as experience from similar cases. As a result, there has been an increase in the number of cases in which cryptocurrency has been successfully traced and seized.

Cases involving crimes against economic order do not typically involve crypto assets, as these are considered financial instruments under current regulations. Criminal law does not list crypto asset services among the subjects of the crime of unauthorized financial activity, which, under the regulations in force

from June 30, 2024, may be performed by financial institutions and investment service providers.[7]

In cases involving budget fraud, the seizure or freezing of cryptocurrencies for the purpose of asset recovery generally serves to secure the confiscation of assets expressed in money. In a large group of such cases, the result is an increase in assets, which represents undeclared and therefore untaxed money, and thus a loss of revenue for the budget. In this way, the state's financial claim can be remedied in criminal proceedings within the framework of monetary confiscation, even in the case of legally acquired assets, through coercive measures ensuring confiscation of assets acquired through criminal activity. In practice, this means that asset tracing extends not only to analog assets, but also to virtual assets, such as cryptocurrencies, typically by searching for identifiable service providers in Hungary and conducting targeted research.

Criminals use a whole range of services and countless variations to conceal the origin of profits from wealth-generating crimes, depending on the size and form of the acquired wealth. Criminal organizations often mobilize their own money laundering infrastructure with front men, money couriers, and crypto mixers, but many criminal groups use professional money laundering services provided specifically for this purpose through so-called matchmaker service providers, who connect criminal organizations wishing to cooperate. Money laundering involving crypto assets largely takes place through underground banking structures, using so-called swapping service providers to guarantee the stability (e.g., conversion to stable coins) and security (e.g., conversion to privacy coins) of crypto assets.

In the case of self-hosted cryptocurrencies, asset tracing targeting crypto assets is carried out during the investigation and examination of seized digital assets. In the case of crypto assets managed by a service provider, it is almost always necessary to contact a foreign service provider in order to identify and secure the asset. Due to the globalization of crime, and money laundering in particular, it is slowly becoming commonplace for investigative authorities and prosecutors to use international channels in order to trace the path of crypto assets, seize assets, or obtain reparations for victims. This usually means contacting the foreign service provider directly. Due to the lack of uniformity in international, European Union, and national regulations, difficulties often arise, for example, in the case of service providers registered in third countries that are unreachable or uncooperative. If judicial cooperation with the authorities of the third country is not possible, efforts to recover assets will be unsuccessful.

7 Hpt. Section 7(3), Bszt. Section 6/A.

The provision of the Be. effective from March 1, 2024 offers a substantive solution to this problem by stipulating that if the subject of the seizure is a claim recorded in the value of electronic data used for payment, and no result can be expected from a request by an economic operator capable of enforcing the suspension of the right of disposal over the seized assets, or the request would involve disproportionate difficulties, the seizure may also be enforced by means of an operation carried out in an information system that prevents the person concerned from disposing of the claim.[8] In practice, this means that if the investigating authority has the correct identification details of the owner of the assets held by the service provider, it can use these details to instruct the service provider to transfer the cryptocurrency to the official wallet. However, several service providers are willing to cooperate both in fulfilling direct data requests and in enforcing coercive measures, and there are also positive examples in the field of international judicial cooperation (Prosecutor General's Office, 2021).

Closing thoughts

The findings of the investigation conducted by the Prosecutor General's Office clearly show that it is essential to develop a uniform and consistent law enforcement practice in relation to cryptocurrencies, in particular their seizure. This is necessary not only within the individual organizational units of the prosecutor's office, but also with regard to the investigating authorities, as the organizations concerned have sought to achieve by issuing a joint circular. This is because both economic crime and the illegal use of cryptocurrencies are subject to constant change, which law enforcement authorities and legislators must monitor and respond to with appropriate measures necessary. For this reason, the Prosecutor General's Office's targeted investigation was followed by a follow-up investigation, the results of which are expected to be available in 2025.

Based on the experiences of the prosecutor's office presented, the main conclusion that can be drawn is that the nature and characteristics of cryptocurrencies pose a significant risk and are increasingly appearing in all types of wealth-generating crimes, including economic crimes; this phenomenon is expected to intensify in the future. In addition, economic criminals are highly adaptable to changes brought about by technological developments, and they exploit the results of these developments, such as cryptocurrencies, in the commission of crimes.

8 Be. Section 328(5).

From the perspective of law enforcement authorities: in the future, it will be crucial to organize joint training courses, compile educational materials, and encourage the development of uniform investigation guidelines in order to secure cryptocurrencies and acquire and develop the necessary competencies. Of course, it is not enough to monitor changes at this level; legislation must also keep pace, and the development of international cooperation is also essential. This is not only a legal issue, but also a matter of social interest, since although crypto assets are intangible, 'invisible' financial instruments, they can cause 'visible' damage if used illegally.

References

Eurojust & European Judicial Cybercrime Network. (2025, March 8). *Crypto assets guide for judicial authorities* (pp. 18-22). Eurojust.

Legfőbb Ügyészség (2021). *Összefoglaló jelentés „Az elektronikus pénz és a virtuális fizetőeszközök – köztük a kriptovaluták – lefoglalásának, illetve zár alá vételének komplex elemzése" témájú célvizsgálatról [Summary report on the targeted investigation entitled 'Complex analysis of the seizure and freezing of electronic money and virtual payment instruments, including cryptocurrencies.']*.

Mezei, P. (2022). NFT-k a szerzői jog világában [NFTs in the world of copyright]. *Iparjogvédelmi és Szerzői Jogi Szemle, 16*(126), 20-24.

Polt, P. (2021). A 21. század kihívásainak hatása a büntetőeljárásra – Kriptovaluták, azaz az új vagyoni értékek büntetőjogi kérdései [The impact of 21st century challenges on criminal proceedings – Cryptocurrencies, i.e. criminal law issues relating to new assets]. In Barabás, A. T. & Christián L. (Szerk.), *Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est* (pp. 419-427). Ludovika Egyetemi Kiadó.

Online links in the article

URL1: *Országgyűlési beszámolók [Parliamentary reports]*. https://ugyeszseg.hu/az-ugyeszseg-rol/orszaggyulesi-beszamolok/

URL2: *Összefoglaló: (EU) 2023/1114 rendelet a kriptoeszközök piacairól [Summary: Regulation (EU) 2023/1114 on markets in crypto-assets]*. https://eur-lex.europa.eu/HU/legal-content/summary/european-crypto-assets-regulation-mica.html

Laws and Regulations

Act CXXXVIII of 2007 on investment firms and commodity exchange service providers and the rules governing their activities

Act CCXXXVII of 2013 on credit institutions and financial enterprises
Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing
Act XC of 2017 on criminal proceedings
Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and Directives 2009/138/EC and 2013/36/EU
Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto assets

Reference of the article according to APA regulation

Nagy, B. G. (2025). Invisible money, visible crime? The emergence of cryptocurrencies in economic crime. *Belügyi Szemle*, *73*(11), 2361–2372. https://doi.org/10.38146/BSZ-AJIA.2025.v73.i11.pp2361-2372

Statements

Conflict of interest

The author has declared no conflict of interest.

Funding

The author did not receive any financial support for researching, writing, and/or publishing this article.

Ethics

No dataset is associated with this article.

Corresponding author

The corresponding author of this article is Bálint Gábor Nagy, who can be contacted at lu@mku.hu.