Comparative Economic Research. Central and Eastern Europe
Volume 29 Number 1, 2026
https://doi.org/10.18778/1508-2008.29.04

Cryptoassets as a Threat to State Sovereignty in the Field of Enforcement and Insolvency

Martin Cahlík https://orcid.org/0009-0001-4025-8941
Mgr., Faculty of Law, Palacký University Olomouc, Olomouc, Czech Republic, e-mail: martin.cahlik01@upol.cz

Simona Kurtinová https://orcid.org/0009-0003-4273-4635
Ing., Faculty of Law, Palacký University Olomouc, Olomouc, Czech Republic, e-mail: simona.kurtinova01@upol.cz

Michal Kozieł https://orcid.org/0000-0001-8561-0358
Ph.D., Faculty of Law, Palacký University Olomouc, Olomouc, Czech Republic, e-mail: michal.koziel@upol.cz

Michael Kohajda https://orcid.org/0000-0001-7235-0921
doc. JUDr., Ph.D., Faculty of Law, Palacký University Olomouc, Olomouc, Czech Republic,
e-mail: michael.kohajda@upol.cz

Abstract

Cryptoassets, as a novel manifestation of financial technology, pose a challenge to traditional legal frameworks, especially in their decentralised nature and the unique way they are held and transferred. Their emergence requires a re-examination of regulatory principles and mechanisms of rights protection in an environment where decentralisation signifies the absence of centralised control. This article examines cryptoassets as a potential threat to state sovereignty within the domains of foreclosure, enforcement, and insolvency. It analyses the legislative challenges arising from the increasing prevalence of cryptoassets and evaluates the applicability of traditional enforcement law instruments to these new technological contexts. This article also integrates empirical findings from the Czech legal environment into the broader theoretical discourse on financial crime and the erosion of state authority caused by decentralised financial systems operating across national jurisdictions Particular attention is devoted to the technical characteristics of cryptoassets, their legal classification, and the practical obstacles encountered in enforcement and insolvency proceedings, especially in situations where debtors refuse or are unable to provide access to their digital assets.
The analysis also incorporates available statistics on enforcement proceedings and evaluates the Czech legal framework governing cryptoassets, focusing on its implications for the effectiveness of enforcement and insolvency processes.

Funding information: M.C. – Faculty of Law, Palacký University Olomouc, Olomouc, Czech Republic; S.K. – Faculty of Law, Palacký University Olomouc, Olomouc, Czech Republic; M.K. – Faculty of Law, Palacký University Olomouc, Olomouc, Czech Republic; M.K. – Faculty of Law, Palacký University Olomouc, Olomouc, Czech Republic.
The percentage share of the Authors in the preparation of the work is: M.C. – 25.00%, S.K. – 25.00%, M.K. – 25.00%, M.K. – 25.00%.
Declaration regarding the use of GAI tools: Not used.
Conflicts of interests: None.
Ethical considerations: The Authors assure of no violations of publication ethics and take full responsibility for the content of the publication.
Received: 5.08.2025. Verified: 20.10.2025. Accepted: 29.01.2026

The research employs both primary and secondary methods, including legal and technical analysis, modelling of real scenarios, and an examination of the relevant legislative instruments.

Keywords: Czech Republic, cryptocurrency, enforcement proceedings, insolvency, legal framework

JEL: K15, K35, K42

Introduction

In recent years, the dynamics of financial markets have changed dramatically with the emergence of new technologies, particularly cryptoassets based on the principle of distributed ledger technology. While traditional enforcement mechanisms through which a right granted by a decision of a state authority is enforced even against the will of the debtor are established in the Czech legal system on the basis of clearly defined institutions of enforcement and enforcement proceedings, licenced enforcement agents (LEAs), in practice, typically deal with assets that are relatively straightforward to seize from a legal perspective. When digital assets are involved, however, enforcing decisions encounters several legal and technical barriers. This contemporary phenomenon which is simultaneously a practical problem represents not only a legislative challenge but also a socio-economic one, as holders of cryptoassets can relatively easily shield their assets from the exercise of state power authority through conventional enforcement procedures.

The main objective of this study is, therefore, to conduct a comprehensive analysis of the applicability of enforcement instruments to intangible movable assets in the form of cryptoassets and, based on a questionnaire survey, to identify obstacles that arise when enforcing decisions against this relatively new category of property. The study employs a combination of qualitative and quantitative research methods. The analysis of legal regulations relevant to enforcement and digital assets plays a central role, both within the framework of national legislation and in the context of European legal standards. In addition, a technical analysis of the operation and security of cryptoassets was conducted to assess their implications for enforcement.

The methodological framework also includes the modelling of practical scenarios that illustrate potential legal and technical complications in the enforcement of cryptoassets. In particular, the paper focuses on the issues of handling hardware and software wallets, as well as the use of PIN codes, seeds, and passphrases. The empirical part of the work is based on a questionnaire survey conducted among LEAs in the Czech Republic, providing direct insights from practice regarding the feasibility of enforcing decisions by targeting cryptoassets. The analysis of the collected data made it possible to identify key problems encountered by LEAs in their professional activities and provided a factual basis for formulating *de lege ferenda* proposals.

Although the empirical analysis focuses on the Czech Republic, the findings have substantial implications for international research. As a European Union (EU) Member State operating under harmonised European regulation (such as the Markets in Crypto-Assets Regulation (MiCA) Regulation and EU anti-money laundering (AML) directives), the Czech experience serves as a critical "stress test" of these supranational frameworks. If enforcement mechanisms fail in a developed jurisdiction with a robust legal tradition purely due to the technical nature

of cryptoassets (e.g., the existence of private wallets or limited international cooperation), it may be concluded that cryptoassets represent a systemic threat to state sovereignty globally. The obstacles identified are not merely local procedural deficiencies but universal challenges that enable financial crime and facilitate the evasion of sanctions irrespective of the jurisdiction.

Cryptoassets as a Threat to State Sovereignty

Cryptoassets, which the European regulator defines as the "digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology" (Regulation (EU) 2023/1114), have recently become the subject of increasing scholarly and public interest. The nature of cryptoassets and the efforts to regulate them have been examined by, for example, Nabilou (2019), Zetzsche, Arner, and Buckley (2020), Ferreira and Sandner (2021), Kohajda and Moravec (2021), and Hrabčák and Štrkolec (2024), Furthermore, numerous studies have addressed regulation within the EU, a particularly active field, notably by Maume (2023), Van Der Linden and Shirazi (2023), and Kozieł (2025), among others.

However, significant challenges arise when addressing the recovery of cryptoassets in the context of enforcing decisions issued by public authorities. Scholarly literature on this topic remains scarce, as it is a relatively new and rapidly evolving area that, given the technological nature and operation of cryptoassets, is difficult for state authorities to effectively comprehend. At the same time, these issues still lie largely beyond the reach of the expert community. We have therefore relied primarily on legislative sources. Since this article focuses on the Czech Republic, particular attention is paid to Czech legal acts and relevant EU legislation.

A growing body of research demonstrates the extensive misuse of cryptoassets for committing financial crimes. Dupuis and Gleason (2020) analyse various methods and mechanisms by which cryptocurrencies can be employed to circumvent regulatory measures and conduct money laundering, identifying specific instruments, 'open doors', used for this purpose. Irwin and Milad (2016) document the early forms of cryptoasset use in the financing of terrorist activities, highlighting the tendency of extremist groups to exploit these technologies as a means of evading conventional financial and supervisory mechanisms. Heyman (2023) identifies key indicators of fraudulent cryptoasset investment schemes and emphasises the need to systematically apply control mechanisms and warning signals (red flag indicators) for the timely detection of high-risk investment structures in the digital financial environment.

Mackenzie (2024) analyses the collapse of major cryptoasset platforms such as FTX and Celsius, where the cult of personality surrounding key executives normalised fraudulent practices. Kabra and Gori (2023) examine the role of organised criminal groups in drug trafficking on crypto-markets, showing that the advantages associated with this mode of trade outweigh potential risks, making it particularly attractive for organised crime. Wronka (2021a) draws attention to the growing risk of circumventing economic sanctions through digital currencies, which poses a threat to international security. In subsequent research, he identifies new challenges for compliance within the decentralised financial ecosystem (Wronka 2021b). Tiwari

et al. (2024) analyse the use of cryptoassets in geopolitical conflicts, demonstrating how both state and non-state actors can employ cryptoassets to evade international sanctions and finance military operations.

These cases show that the issue of law enforcement in the domain of cryptoassets is not merely a technical or legal challenge, but rather represents a serious threat to state sovereignty over financial flow control and the enforcement of law. Building on the analysis of the Binance case – where the exchange was convicted by U.S. authorities of serious financial crimes, including money laundering and terrorism financing – Cardao-Pito (2025) formulates two fundamental hypotheses concerning the relationship between cryptocurrency exchanges and state sovereignty:

H1: Cryptocurrency exchange organisations can represent a threat to national states because their power to issue assets with properties akin to money may result in the unchecked depletion of the means available for states' lawful financial sanctions over these exchanges.

H2: Cryptocurrency exchange organisations can pose a threat to national states because their ability to issue assets with properties akin to money may result in the unchecked acquisition of resources, allowing them to compete with national states.

These hypotheses are particularly relevant to the issue of enforcement proceedings in the Czech Republic. The first hypothesis suggests that the ability to issue cryptoassets enables debtors to create parallel financial systems beyond the reach of traditional enforcement mechanisms. While the state invests significant resources in building and maintaining its enforcement apparatus, debtors can relatively easily transfer their assets into cryptoassets or use cryptoassets as money, thereby effectively neutralising state or international sanctions.

The second hypothesis highlights a deeper problem: cryptoassets not only allow individuals and entities to evade sanctions but also provide the means for building alternative power structures and establishing markets beyond the supervision of state authorities. In extreme cases, entities holding substantial amounts of cryptoassets may finance their own security forces, infrastructure, or even compete with the state for control over certain territories or sectors of the economy.

Within the context of the Czech legal system, these hypotheses acquire a practical dimension. As our model cases illustrate, a debtor possessing cryptoassets can, in effect, decide whether or not to cooperate with the enforcement agent. Although this article primarily focuses on natural persons rather than legal entities, it is also necessary to point out the potential threat posed by legal persons such as cryptocurrency exchanges or other companies that hold cryptoassets. They may exploit the potential of cryptoassets to position themselves in parity with state power. The absence of effective coercive instruments means that the state monopoly on legitimate force, which forms the cornerstone of modern statehood, is significantly weakened in the sphere of cryptoassets.

The general cases concerning natural persons described later in this article are also applicable to legal entities; however, such entities usually possess considerably greater personnel, as well as infrastructural and financial capacity to use cryptoassets in other ways. As Cardao-Pito (2025)

notes, one of these ways is to create assets (cryptoassets or stablecoins) with properties analogous to money, over which the state has no effective means of seizure or freezing.

European Dimension

A key milestone in the EU's Regulation on Markets in Cryptoassets (Regulation (EU) 2023/1114), which entered into force on 29 June 2023 and became fully applicable on 30 December 2024. This pivotal regulation represents the first comprehensive attempt to harmonise cryptoasset regulation at the supranational level. Its primary objective is to ensure legal certainty and promote innovation while protecting consumers and financial stability. It does so by requiring providers of cryptoasset services and other entities operating in this market to obtain authorisation or a licence from the supervisory authority of an EU Member State.

A key consequence is the European regulator's requirement that service cryptoasset providers must have their registered office within a Member State of the European Union. This ensures that they remain under the close supervision of both national regulators and the EU as a whole. However, from the perspective of this article, even more significant legislation is the implementation of the Regulation of the European Parliament and of the Council (EU) 2023/1113, which obliges cryptoasset service providers to collect essential identifying data of the parties involved in each cryptocurrency transaction and to verify the ownership of crypto wallets. Both types of information are crucial for subsequent audits in tax, criminal, or private-law contexts.

The regulation also devotes considerable attention to stablecoins. Although they represent a smaller share of the cryptoasset market, their importance is fundamental, as they serve as a medium of exchange and a store of value within the cryptocurrency ecosystem. Unlike central bank digital currencies, which constitute a direct digital form of a national currency, stablecoins are issued by private entities, and their value is pegged to a fiat currency, most commonly the U.S. dollar. This similarity to traditional money is the reason why the MiCA Regulation (Regulation (EU) 2023/1113) imposes stricter rules on them than on other cryptoassets. The regulation establishes limits on transaction volumes, mandates the redemption of tokens at full nominal value, and prohibits the payment of interest to prevent their speculative use. These measures aim to strengthen the stability of stablecoins, enhance consumer protection, and avert the risk that they could disrupt the EU's monetary policy or financial stability.

Although this represents a major step forward in the regulation of cryptoassets at the EU level, there is still no European legislation requiring providers of cryptoasset-related services to cooperate with the state authorities of a Member State other than the one in which they have their registered office, even if they operate within that country.

A similar problem to the one discussed in this article can also be identified in Poland, a country closely related to the Czech Republic both in terms of social development and legal tradition. Poland is likewise seeking ways to enforce cryptoassets as efficiently as possible. The starting point for Polish legal theory and practice is the definition of a cryptoasset as a property right, established by the jurisprudence of the Polish Supreme Administrative Court (Judgment of the Supreme Administrative Court of 6 March 2018). From this interpretation, it follows that

a cryptoasset may be subject to enforcement under Article 909 et seq. of the Polish Code of Civil Procedure (Act of 17 November 1964 – Code of Civil Procedure).

According to Article 801–1 of the Polish Code of Civil Procedure, the debtor is obliged to submit to the enforcement officer, either orally for the record or in writing, an inventory of assets together with a declaration of its accuracy and completeness, under the threat of criminal prosecution for making a false statement. However, a similar problem arises here as in most EU Member States: if the debtor fails to cooperate with the enforcement officer, the latter has, apart from the threat of criminal prosecution, very limited means to compel the debtor to disclose access codes or surrender a hardware wallet.

If the cryptoassets are held on an exchange, the situation is analogous to that in the Czech Republic, as the procedure follows the unified framework of European legislation. In such cases, the enforcement officer may request the exchange to block the debtor's cryptoassets in their account, and the exchange is obliged to cooperate with and comply with the enforcement officer's request.

We are aware that this journal focuses on comparative studies; however, given that the situation in each Member State is highly specific and that a direct comparison of the issues examined here would far exceed the permissible length of the article, we have chosen to concentrate primarily on enforcement and insolvency proceedings in the Czech Republic. This focus is further justified by the fact that the questionnaire survey was conducted in the Czech Republic among Czech enforcement agents; therefore, the present study primarily addresses the Czech context, which best corresponds to the data obtained.

Our objective is thus mainly to highlight the specific features of the Czech system, which may subsequently serve as a source of inspiration for other jurisdictions when addressing similar issues already resolved in the Czech Republic. More importantly, we hope the example of insufficient Czech solutions will stimulate a Europe-wide expert discussion that will lead to or at least contribute to the establishment of unified rules within the EU.

As regards the actual enforcement of decisions, two basic scenarios can be distinguished in general terms. The first scenario concerns a debtor who holds cryptoassets recorded in some manner on a regulated exchange (for example, through an account with an entity subject to European regulation). In this case, the rules are harmonised within the EU. Centralised cryptoasset exchanges are obliged to maintain relatively detailed records of their clients. Theoretically, this gives the state a more straightforward position, since the enforcement of cryptoassets in this context closely resembles the enforcement of ordinary financial funds held in bank accounts. In practice, however, numerous practical limitations persist, most notably the continuing inadequacy of international cooperation in this field.

For example, Czech enforcement agents reported in the questionnaires that foreign exchanges often fail to respond to their inquiries regarding the existence of a debtor's account. At this point, the most feasible approach involves cooperation through national regulators supervising exchanges in the respective jurisdictions. The remaining rules arising from the MiCA Regulation

or AML measures are uniform across the EU, as they have been adopted in the form of directly applicable regulations.

The second enforcement scenario is considerably more complex (as we illustrate further using the example of the Czech Republic). If the debtor holds their cryptoassets in a private hardware wallet, then without the debtor's cooperation, under current legal instruments, the state's enforcement capabilities are limited or non-existent. At present, all EU Member States face the same or similar challenges and continue to seek appropriate solutions, thus far without success.

Enforcement Proceedings and Other Forms of Enforcement in the Czech Legal System

Enforcement, the final stage of the civil process that involves the compulsory enforcement of a right granted by a court, is based on a duality of legal frameworks in the Czech legal system.

The enforcement of a decision represents the older form of enforcement and is regulated by Section 251 of Act No. 99/1963 Coll., the Code of Civil Procedure. It constitutes judicial enforcement, meaning that enforcement is ordered and executed directly by a judicial authority. This form of enforcement is, however, a somewhat rigid instrument, used in practice only in specific legal cases or situations where no other method of enforcement is available.

By contrast, enforcement proceedings represent a newer form of enforcement, governed by Act No. 120/2001 Coll., the Enforcement Code. In this case, enforcement is carried out by a private business owner – a natural person authorised by the state to operate an enforcement office who is thus empowered both to order and to perform enforcement independently (Act No. 120/2001 Coll., § 1 (1)). This person is designated as an LEA and must be of good moral character and integrity, hold a university degree in law (or an equivalent degree in the field of legal sciences), have at least three years of professional practice in enforcement activities, and successfully pass the enforcement agent's examination (Act No. 120/2001 Coll., § 9 (1)).

Both forms of enforcement require the existence of an enforcement title (Act No. 99/1963 Coll., § 261 (2); Act No. 120/2001 Coll., § 37 (2)), i.e., a decision or another title expressly defined by law (or a similar decision), accompanied by a confirmation of enforceability issued by the competent authority. Enforcement titles are largely identical under both legal regimes, although the enforcement of a decision may also rely on historically obsolete titles (e.g., enforceable decisions of state notaries). The Enforcement Code titles are broadly defined as "an enforceable decision of a court or other authority active in criminal proceedings, if it grants a right or affects property, an enforceable decision of a court or licenced enforcement agents, if it grants a right, obliges to an obligation or affects property, an enforceable arbitration award, a notarial deed with permission for enforcement, an enforceable decision and another enforcement title of a public authority and other enforceable decisions and approved settlements and documents, the enforcement of which is permitted by law" (Act No. 120/2001 Coll., § 40 (1)). The enforcement

of a decision may be initiated based on similar enforcement titles, provided that they are designated as such by law.

However, decisions issued in administrative or tax proceedings are excluded from judicial enforcement. It is therefore impossible to order or execute enforcement based on these titles within that framework (Act No. 99/1963 Coll., § 274 (1)). This limitation, however, does not apply under the Enforcement Code, meaning that such decisions can, in principle, be enforced through enforcement proceedings. Nevertheless, such cases are relatively rare, since administrative and tax enforcement are governed by their own special procedures, which are generally more suitable for enforcing such decisions. It is anticipated that the limitations on enforcing cryptoassets within administrative or tax proceedings will be similar to those encountered in enforcement proceedings or the judicial enforcement of decisions.

In both enforcement proceedings and the enforcement of a decision, enforcement is initiated exclusively at the request of the person entitled under the enforcement title. Thus, there is no automatic stage within the Czech civil process that compels the debtor to comply voluntarily with the decision.

Under the Enforcement Code, the process begins with an enforcement motion that must designate the LEA who will carry out the enforcement. The motion must satisfy the general requirements applicable to submissions: it must specify the petitioner, the subject matter, and the relief sought, and it must be duly signed and dated. It is also necessary to identify the debtor (i.e., the obligor), state the obligation to be enforced, and precisely indicate the enforcement title (Act No. 120/2001 Coll., § 38 (1)). Once the LEA selected by the entitled person who may freely choose from all LEAs in the Czech Republic – receives authorisation from the competent court, the agent performs almost all procedural acts independently, without further cooperation from the entitled party, including determining the method by which the enforcement will be executed.

Under the Code of Civil Procedure, enforcement follows largely the same principles, but with key differences. When enforcing a monetary obligation, the motion must also specify the method of enforcement for example (e.g., wage deductions, garnishment of receivables, or the sale of movable or immovable property) (Act No. 99/1963 Coll., § 258 (1), § 261 (1)) This requirement, which is fundamental for the seizure of cryptoassets, considerably reduces the suitability of judicial enforcement for such cases. When dealing with a monetary claim, the entitled party usually selects a method likely to yield liquid assets. Therefore, without any other information about the debtor, they will most likely propose the sale of movable property as an *ultima ratio* method of enforcement.

It should also be noted that even if the application for enforcement lists all methods of enforcement, it is unlikely to succeed, since both the court and the bailiff must act in accordance with the principle of proportionality, proceeding from less intrusive means (such as wage deductions) to those capable of affecting a broader range of the debtor's property. Moreover, if the debtor does not personally hold the cryptoassets, the application must specify the person or entity that holds them. Unlike LEAs, courts and judicial bailiffs lack specialised instruments

to locate or seize cryptoassets, which makes the choice of judicial enforcement highly inefficient when the debtor is presumed to own such assets.

It should further be emphasised that, in the case of judicial enforcement, the applicant cannot choose any court to order and carry out the enforcement; jurisdiction lies exclusively with the debtor's general court, i.e. the court in whose district the debtor has their place of residence or registered office. Thus, if the entitled party opts for this rigid form of enforcement, disregarding the aforementioned procedural and practical obstacles, they will ultimately face the same limitations as those encountered by LEAs in enforcement proceedings. The individual cases discussed below will therefore illustrate problems that are, at least theoretically, identical across both forms of enforcement.

Current Enforcement Trends in the Czech Republic

Recent enforcement proceedings in the Czech Republic reveal concerning trends that merit attention in the context of the interaction between traditional enforcement mechanisms and emerging technologies such as cryptoassets. According to publicly available statistics for 2024, approximately 3.3 million enforcement proceedings were initiated in the Czech Republic, reflecting the extensive reliance of the enforcement apparatus. This considerable volume of enforcement activity poses not only administrative challenges for the state but also significant socio-economic consequences for the population.

The financial dimension of these enforcement proceedings illustrates their economic significance. Enforcement authorities have recovered roughly CZK 568 billion (approximately EUR 22 billion), demonstrating the magnitude of the financial flows subject to state enforcement powers. Notably, the average amount per enforcement proceeding stands at CZK 922,615 (approximately EUR 36,700) (Institut prevence a řešení předlužení, 2025a). This figure substantially exceeds the country's annual gross average wage (CZK 590,748, or around EUR 23,500) (Český statistický úřad, 2025), indicating a systemic debt trap rather than isolated cases of insolvency.

An age-based analysis further reveals that the enforcement burden is most pronounced in the working-age population, peaking in the 45–49 age group (over 80,000 individuals), and significantly affecting those aged 35–54 (Exekutorská komora České republiky, 2025). Geographically, strong regional disparities persist: while north-western regions record enforcement rates of up to 12.8%, central parts of the country show values below 4%. This uneven distribution suggests that the socio-economic factors driving enforcement are territorially concentrated (Institut prevence a řešení předlužení, 2025b).

Although the trend between 2022 and 2025 shows a modest decline from 7.5 to 6.6% in the overall proportion of individuals under enforcement (Institut prevence a řešení předlužení, 2025c), the share of multiple enforcement proceedings remains persistently high at 76–77% (Institut prevence a řešení předlužení, 2025d). The decrease in the total number of individuals enforcement cases since 2023 is primarily attributable to the entry into force of Amendment No. 286/2021 (Part 2, Amendment Point 94), which introduced the institution of terminating "unsuccessful enforcements". This legislative measure allows for the discontinuation of enforcement proceedings

once two cumulative conditions are met: (1) the absence of any recovery sufficient to cover the enforcement costs during the previous six years, and (2) the absence of any seizure of the immovable property within the given enforcement proceedings.

These data provide essential context for discussing cryptoassets. Individuals facing significant enforcement pressure may be increasingly inclined to seek alternative financial instruments beyond the reach of traditional enforcement mechanisms, thereby creating new regulatory challenges at the intersection of digital technologies and legal enforcement. The statistical analysis of enforcement proceedings in the Czech Republic thus provides a crucial socio-economic background for assessing the enforceability of cryptoassets. Given the sheer number of enforcement cases, as well as their economic magnitude and structural nature, the issue of digital-asset enforceability is becoming increasingly relevant. High levels of indebtedness and the prevalence of multiple enforcement proceedings exert strong pressure on debtors, who may perceive cryptoassets as a means of shielding part of their assets from enforcement sanctions.

Cryptoassets as a Matter of Law

When considering the enforcement of cryptoassets, it is first necessary to determine their legal nature under Czech law. For an object to quality as a "thing" in the legal sense within the meaning of the Czech Civil Code, it must cumulatively meet two legal characteristics: it must be distinct from a person and must serve human needs (Act No. 89/2012 Coll., § 489). The Code also contains a negative definition, expressly providing that a thing is not the human body or its parts, and that living animals are likewise not regarded as things. These entities are therefore explicitly excluded from the concept of a "thing". Cryptoassets do not fall into any of these excluded categories and thus satisfy the first requirement – their distinctness from a person – without difficulty. The analysis must therefore focus on the second requirement, namely whether cryptoassets can "serve human needs" within the meaning of the Civil Code.

Legal theory further supplements this definition by adding an essential attribute namely, that a thing must be capable of being the object of subjective property rights, particularly the right of ownership (Dvořák, Švestka, and Zuklínová 2006:377). This requirement may be derived indirectly from the Civil Code's definition of a tangible thing as a controllable part of the external world that possesses the character of an independent object (Act No. 89/2012 Coll., § 496 (1)). It logically follows that an object which cannot be controlled cannot serve as the object of private property rights and therefore cannot qualify as a thing within the meaning of the Civil Code, even if it exists as a physical entity.

When assessing these conditions, it is evident that cryptoassets are neither natural persons (§ 23) nor legal persons (§ 118) under the Civil Code. Furthermore, they demonstrably serve human needs, and their utility is further corroborated by legal definitions, for instance, in the European Regulation on cryptoassets, which Czech law incorporates by reference. Section 4 (8) of Act No. 253/2008 Coll., on specific measures against the legalisation of proceeds from crime and the financing of terrorism refers to the European Regulation on cryptoassets, which defines them as "a digital representation of value or a right that can be transferred or stored electronically using distributed ledger technology or similar technology" (Regulation (EU) 2023/1114, Article 3 (1)(5)).

Cryptoassets also satisfy the third and final criterion for classification as a legal "thing": they are capable of constituting the object of subjective property rights, as they can be possessed, transferred, or traded. From a legal standpoint, having satisfied all three cumulative requirements (distinct from a person, serving human needs, and being capable of holding private property rights), cryptoassets therefore qualify as "things" under the Civil Code. This conclusion is supported by the interpretation of Section 489, which encompasses a wide range of tangible and intangible objects within its broad definition. The current Civil Code deliberately adopts a more comprehensive conception of "thing" than previous legal regulations, drawing on pre-war Czechoslovak jurisprudence and expressly departing from the narrowly materialistic understanding that is characteristic of the twentieth century. According to Section 489, "things" include both tangible and intangible objects, such as industrial property rights, book-entry securities, and various financial instruments.

Regarding the classification of property as tangible or intangible, unlike fiat currencies, cryptoassets have no physical counterpart. They exist exclusively in a decentralised digital environment without territorial boundaries. Their existence depends on the technological infrastructure of distributed networks, which facilitates nearly instantaneous and cost-effective international transfers of value without the involvement of the traditional banking system. The technological foundation of these innovative financial instruments lies in distributed ledger technology, which fundamentally alters the methods of storing and sharing information. Unlike centralised database systems managed by a single authority, distributed ledger technology enables the distribution and synchronisation of data across multiple computer nodes without reliance on a central repository.

Pursuant to Section 498 (1) of the Civil Code, immovable property comprises land, underground structures with a specific purpose, property rights relating thereto, and rights that are expressly designated by law as immovable property. All other objects, whether tangible or intangible, are deemed movable. In light of these considerations, cryptoassets must be classified as intangible movable property under private law (Act No. 89/2012 Coll., § 496). They may also be regarded as fungible (i.e., that one unit of the cryptoasset is interchangeable with any other unit of the same type).

Based on the foregoing analysis of the legal nature of cryptoassets in relation to the provisions of the Enforcement Code, several fundamental conclusions may be drawn for enforcement proceedings. Since cryptoassets satisfy the requirements for classification as intangible movable property under the Civil Code, they fall within the scope of enforcement under Section 59 (1) (c) of the Enforcement Code, i.e., by way of the sale of movable property. This means that, when enforcing a monetary claim, an LEA may seize a debtor's cryptoassets in the same manner as other movable property in its possession. Nevertheless, the technical specificities of cryptoassets present substantial practical challenges for enforcement proceedings, which will be further illustrated in the following model situations.

Challenges in the enforcement of Cryptoassets

The technological characteristics of cryptoassets pose fundamental challenges for their enforcement proceedings. Unlike traditional financial instruments tied to a specific regulatory and geographical framework, cryptoassets exist in a decentralised digital environment beyond state borders. Their architecture, based on the technological infrastructure of distributed networks, enables almost immediate and cost-effective international value transfers without involving the traditional banking system. Additionally, the person who developed a particular cryptoasset usually has no right, or even the ability, to intervene in this technological system and, therefore, cannot respond to any calls for cooperation or to freeze or seize cryptoassets. This aspect disrupts the established financial flow principles and presents new challenges for enforcement authorities and current legislation. Cryptoassets are usually based on three basic factors:

1. A form of distributed ledger technology (DLT) technology that allows information to be stored via a distributed ledger.
2. Cryptographic information security and identity verification that uses asymmetric cryptography.
3. Decentralisation.

A distributed ledger based on DLT technology allows information to be stored, processed, and recreated anywhere in the world. It uses a decentralised system of users who, if they meet the requirements of the network on which the distributed ledger is maintained, and can process and store information in the distributed ledger for some form of reward. Once the information is stored, other users verify its authenticity based on predetermined criteria and synchronise their distributed ledger with this new information. It is therefore clear that no central entity would authoritatively decide what information will be on the network or how it will be handled. Still, it is necessary for all users processing this information to agree to this.

All information on the network of individual cryptoassets is then encrypted so that the content of the information is known only to the parties concerned, i.e., the person who created the information and the people to whom it was sent. This is done using asymmetric cryptography, a technology where the sender encrypts information using a public key, and the recipient can only decrypt it using their corresponding private key.

Cryptoassets are stored in "crypto wallets", which are categorised as either hot or cold. Hot wallets are constantly connected to the internet and exist only as a specific type of software. Cold Crypto wallets (e.g., Trezor or Ledger) are physical devices whose software connects to the Internet only when a transaction is made (Takei and Shudo 2024:747–765). A crypto wallet has a public identifier, known as a public address, for third parties. A public address can be likened to a bank account number; it is usually a public key that is modified using mathematical operations (hashing). For example, the public address of the first Bitcoin wallet belonging to Satoshi Nakamoto is: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa.

The security of these crypto wallets is also based on asymmetric cryptography, where the public key verifies you as the owner of the public address to which you can send or receive cryptoassets

(Xu, Weber, and Staples 2019:30–31). The private key serves as a password to access the crypto wallet; without it, neither the wallet nor the cryptoassets stored within can be controlled. Above the private key is a "superior master key" a recovery phrase called a "seed". This phrase comprises twelve or twenty-four words (Kaliský 2018:40), from which the private key is subsequently derived. The seed is created when the wallet is generated, and it must be recorded on a reliable medium or memorised. If the user forgets the private key, the wallet can be restored using the seed by correctly entering the words in the original order. If the seed is forgotten, there is almost zero chance of reassembling it and restoring the crypto wallet.

While crypto wallets incorporate robust security, two additional features are key in enforcement proceedings. The first is the PIN, which can be set for cold wallets. This numeric combination must be entered before the user can operate the wallet. If the user forgets the PIN, they cannot connect to the wallet, but access to the cryptoassets is still possible using the seed. If the PIN is entered incorrectly, the time delay for re-entering the PIN usually doubles, but only up to a point when the wallet's contents are completely erased, forcing recovery solely via the seed.

The most problematic security feature from the point of view of enforcement proceedings is the passphrase technology (loosely translated as "access phrases"), which allows the user to add additional and primarily custom words to the seed. This process creates a secondary cold wallet that can be restored using both the seed and the passphrase. If a user moves all their cryptoassets to this new crypto wallet with a passphrase, no other user can obtain the cryptoassets without knowing the phrase, even if they know the seed. The passphrase is not stored on the crypto wallet itself, but on the chip of this wallet, meaning that even if someone gains unauthorised access to the crypto wallet, they will not find this passphrase.

In the context of recovering cryptoassets, the provisions of Section 58 of the Enforcement Code are both extremely important and highly problematic. The law exhaustively defines the methods of enforcement but does not explicitly mention the seizure of cryptoassets as a distinct method. This raises the first significant legal question: under which existing method can cryptoassets be classified? The most likely classifications are under Section 58 (2)(b) as "severance of other property rights" or under Section 58 (2)(c) as "sale of movables", given their character as intangible movables. However, this classification runs counter to the technological specifics of cryptoassets, particularly their decentralised nature and the method of securing them through asymmetric cryptography.

The legal provision also establishes a sequential order of enforcement methods, with the seizure of other property rights or the sale of movables used only after less invasive methods have been exhausted. This procedure may complicate the timely seizure of cryptoassets, which can be quickly transferred to other addresses or exchanged for other assets. The time delay imposed by the legal order may ultimately prevent the effective seizure of cryptoassets, as the debtor has enough time to move them out of the enforcement agent's reach. A special problem is also posed by the provision of Section 58 (1), which limits the seizure of assets to the extent that it is "safely sufficient" to cover the claim being enforced and the related costs. For cryptoassets, whose value can fluctuate significantly, it is difficult to determine a safe and sufficient extent, which may lead to excessive or insufficient seizure due to market volatility. However, it is very likely that "market volatility" will

be the very reason under which "safely sufficient" seizure will be subordinated. Therefore, it will be irrelevant whether the bailiff seizes more than the claims and the costs of conducting the enforcement. However, after paying the claim and the costs of conducting the enforcement, the LEA will be forced to return the remaining portion of the funds they collect from the sale of cryptoassets to the debtor. In addition, debtors may intentionally disperse their cryptoassets among many wallets with small balances, thereby making comprehensive seizure more difficult and reducing enforcement efficiency due to the costs of securing them.

Due to the nature of cryptoassets, proving debtor ownership may be difficult, especially if the cryptoassets were acquired through foreign cryptocurrency exchanges or decentralized finance (DeFi), which is a relatively common phenomenon. The possibility of establishing the existence of such assets is significantly limited in enforcement proceedings. In addition, cryptoassets are often held in anonymous wallets, in wallets of foreign cryptocurrency exchanges outside the Czech Republic's jurisdiction, or in completely autonomous and independent systems.

In enforcement proceedings, the debtor may be requested to provide information about their assets, including cryptoassets. Cooperation from a third party, such as a domestic cryptocurrency exchange or digital asset provider, may also be requested. However, even if the existence of cryptoassets is established, there is no guarantee that they will be effectively secured, let alone sold in enforcement proceedings. If the assets are stored on foreign platforms, asserting a claim against those entities is impossible from the perspectives of both the Czech legal system and European standards. In that case, it is legally very complex and financially costly. The absence of specific legal standards governing the enforcement of cryptoassets, combined with the higher costs and time-consuming enforcement processes associated with them, makes the entire procedure considerably inefficient and, in many cases, practically unfeasible.

One of the key aspects of successful asset recovery is not only their acquisition but also their subsequent safekeeping (Act No. 120/2001 Coll., § 46 (5)). For example, Erp (2022:22–25) emphasises that, after obtaining control over cryptoassets (either by obtaining a private key or by direct transfer), the LEA must securely deposit these assets in a separate wallet that functions as a trust account. This specific wallet must ensure the separation of the secured cryptoassets from other assets and protect them against possible further enforcement, a crucial technical and procedural aspect of managing cryptoassets in the enforcement proceedings. If it is impossible to store cryptoassets in a hardware wallet, the LEA is forced to secure a specialised custodian to ensure the custody of these cryptoassets for the LEA; however, this procedure will increase the cost of securing assets during enforcement.

In this context, LEAs must acquire and further develop a deep and comprehensive knowledge of the technologies behind cryptoassets, which is key to effective enforcement. From a procedural perspective, LEAs must also develop and implement standardised procedures for handling digital assets that reflect their specific nature, which is different from traditional forms of property. This includes, among other things, a documented process for receiving, storing, and subsequently transferring cryptoassets, including consistent logging of all operations to ensure transparency of the entire process. It is also necessary to ensure the careful and comprehensive handling of these cryptoassets within the framework of internal and external processes

related to the transfer of cryptoassets between individual crypto-wallets, since a single error when transferring cryptoassets can mean absolute loss, leading to the financial liability of the LEA for this damage caused.

If the LEA manages to recover the relevant units of cryptoassets, another potentially problematic process comes into play: their subsequent monetisation. The current practice of other state authorities[1] is to sell the received cryptoassets in the form of an auction, which is preceded by the publication of the auction decree. Although this method achieves the desired result, it also introduces many uncertainties that can be fundamental to the process.

The first issue is determining the lowest bid. Current practice tends to leave the lowest bid undefined, linking it to the asset's value at a specific time at an electronic address on the Internet. Specifically, it is possible to identify the determination of the lowest bid as "the amount of the XBP index at 8:00 a.m. CET on the day the auction begins within the meaning of Article 8, paragraph 9 of the Auction Rules" (Daňhel 2025: 3). The price at this specific moment may already be significantly below (or above) the price stated in the item list. Conversely, after the auction, the bidder remains in a state of uncertainty for a relatively significant period as to when the movable property will arrive in their electronic wallet. Given the relatively high volatility in cryptoasset markets, this time lag can be a significant problem for the bidder. It is also highly likely that the bidder will not receive the full amount of the cryptoasset offered, as it will always be reduced by the blockchain transaction fee, which can be highly variable depending on the type of cryptoasset. However, since private sales are not permitted in this case, an auction is the only possible method.

As demonstrated by the growing body of research on financial crime associated with cryptoassets, law enforcement in this area is not merely a matter of legislative gaps but represents a complex institutional and technological challenge. The successful enforcement of cryptoassets requires far more than an adequate legal framework; it demands specialised human resources, advanced technologies, and international coordination.

For instance, European Commissioner Mairead McGuinness has repeatedly emphasised the need for cross-border collaboration and the harmonisation of regulatory approaches (Jones 2023). The Bank for International Settlements similarly notes that the global nature of cryptoassets poses challenges that necessitate coordinated regulatory action. Where regulatory gaps and inconsistencies exist between jurisdictions, the associated risks cannot be fully mitigated (Ocampo, Branzoli, and Cusmano 2023).

Morton (2020) advocates for the establishment of a unified system of regulatory rules and competent supervisory authorities, recommending that such institutions be vested with the power to impose sanctions and criminal penalties to strengthen cybersecurity and combat illicit activities involving cryptoassets. As Cardao-Pito (2025) points out, the successful enforcement of cryptoassets in criminal proceedings requires specialised police units that are sufficiently trained and equipped with the technological tools and resources necessary to combat financial crime. Enforcement agents in the Czech Republic currently lack these capacities to a sufficient extent.

1 In this case, the Ministry of Justice of the Czech Republic.

Effective enforcement of cryptoassets, therefore, requires not only legislative reforms but also investments in technological infrastructure enabling the tracking of blockchain transactions, enhanced international cooperation (since cryptoassets by their very nature transcend national jurisdictions), and continuous professional training of LEAs in this rapidly evolving field. Without these institutional and technological capacities, even the most sophisticated legislative provisions will remain a *lex imperfecta* a dead letter of the law.

Model Cases That May Arise When Executing Cryptoasset Decisions

The following scenarios outline several model situations that may arise during enforcement proceedings in which cryptoassets will be affected. For these models, we assume that the LEA makes all possible legal efforts to satisfy the creditor's claim and the debtor has no other assets; therefore, any primary enforcement order has been unsuccessful.

Model situation No. 1

Filip is a long-time investor in speculative cryptoassets, which he regularly buys for cash at a Bitcoin ATM and transfers to the public address of his digital crypto wallet. He has no information stored and remembers his seed. Filip is subject to enforcement proceedings and, when requested to declare his assets, denies ownership of the cryptoassets.

This situation is relatively straightforward. Since the debtor did not declare ownership of the cryptoassets in the asset declaration and the cryptoassets are stored in a digital crypto-wallet, the LEA has no way of knowing about their existence and, consequently, cannot order or carry out the enforcement. If Filip purchased the cryptoassets through his bank account, it is possible that the bailiff could identify the cryptoassets using a bank statement. Still, recovery would likely still be impossible.

Model situation No. 2

Filip is a long-time investor in speculative cryptoassets, which he regularly buys in cash at a Bitcoin ATM and transfers them to the public address of his hardware crypto wallet, which is physically located at his residence. He does not have any information stored about this wallet; he remembers his seed and has set a PIN on the crypto wallet. Filip is subject to enforcement and, when requested to declare his assets, denies ownership of the cryptoassets.

Within model situation No. 2, it is possible to consider the following options:

- *Variation 2.1: Filip has his seed written on a piece of paper, which he does not keep with his wallet. A PIN does not protect the crypto wallet.*
- *Variation 2.2: Filip has his seed written on a piece of paper that he does not keep with his wallet. The crypto wallet is protected by a PIN that Filip has not stated anywhere.*
- *Variation 2.3: Filip has his seed written on a piece of paper (but also memorised), which he keeps next to his crypto wallet. He also has his PIN written next to the seed.*

- *Variation 2.4: Filip has his seed written on a piece of paper that he keeps near his crypto wallet. He also has his PIN written next to the seed, but Filip has a set passphrase in his head, which secures all cryptoassets in a hidden wallet.*
- *Variation 2.5: Filip's hardware wallet is not located at Filip's residence.*

This situation differs from Model Situation No. 1. In the event of a movable enforcement, the LEA may find the hardware wallet, label it with a sticker, and ensure its transport to the enforcement warehouse. However, this transfer only occurs after the specified period has elapsed, allowing the debtor an opportunity to dispose of the cryptoassets, although he should not do this.

A complex situation then arises: the LEA possesses the crypto wallet (which holds access to the cryptoassets), but lacks the ability to dispose of the cryptoassets. After all, he does not know the PIN or the seed required for restoration. At this stage, the LEA has three basic options: a) invite the debtor to provide the PIN, b) invite the debtor to provide the seed, and c) set the crypto wallet to factory settings.

If the debtor refuses to provide the PIN or seed, the LEA can impose administrative fines until the information is provided. However, the debtor can simply tell the LEA that he does not remember either key. In that event, the LEA has no choice but to reset the crypto wallet and sell it for its usual value.

Variation 2.1 offers the potential for the first successful enforcement. Upon seizing the wallet and finding the seed, the LEA can transfer the cryptoassets to their own hardware (or other) crypto wallet and proceed to auction them.

Variation 2.2 offers the potential for a second successful enforcement. Once the LEA has performed all the actions within the movable enforcement, they can bypass the PIN on the hardware wallet by restoring the wallet (or cryptoassets) to another wallet using the seed, and then auction the assets.

Variation 2.3 follows the same procedure as the previous two variations, offering another successful enforcement possibility.

However, it is important to note that in scenarios 2.1–2.3, an alert and quick debtor can still outrun the LEA and restore the cryptoassets by using the seed, even without the physical crypto wallet. If the agent discovers the seed was used and the cryptoassets are elsewhere, they revert to the difficulties of the general model situation No. 2. While criminal sanctions are theoretically possible for the debtor, the creditor may gain nothing from either the enforcement or criminal proceedings.

Variation 2.4 is similar to Variation 2.3, but includes the complicating factor of the passphrase. Even though the LEA seizes all essential components (crypto wallet, PIN, and seed), they only gain access to the empty "basic" wallet. The assets remain secured in the hidden wallet, which is accessible only after entering the passphrase. The LEA cannot recover the assets by restoring the cryptoassets to another wallet since they still do not know the passphrase, a mandatory prerequisite for successfully restoring cryptoassets to a newly created (or existing) crypto wallet.

The agent is again forced to rely on the debtor's cooperation or merely monetise the hardware wallet device.

Variation 2.5 is almost certainly destined to fail. Since the LEA does not have any information about the debtor's ownership of cryptoassets, there is no possibility of seizing the debtor's cryptoassets or imposing recourse for the debtor's non-cooperation during the enforcement.

Model situation No. 3

Filip is a long-time investor in speculative cryptoassets. He regularly buys these cryptoassets on a cryptocurrency exchange and leaves them in the exchange's electronic wallet. Filip is subject to enforcement and, when requested to declare his assets, denies ownership of the cryptoassets.

This option represents "the light at the end of the tunnel" for the LEA, as there is a relatively easy and realistic way to access and obtain cryptoassets. The core strategy involves the agent sending a request for cooperation to the domestic exchange office. This request invites the exchange to disclose whether Filip has an account, including an electronic wallet, data on this electronic wallet and data on the debtor's cryptoassets that are on the electronic wallet. If the exchange cooperates, the LEA can enforce the seizure of those assets and monetise them. However, a fundamental problem persists: the debtor's ability to dispose of the assets. An enforcement order might be served too late, or the data in the enforcement order may no longer correspond to the real balance on the debtor's electronic wallet.

Data from Licensed Enforcement Agents

As part of the research, we surveyed LEAs by sending a questionnaire through the Chamber of Licensed Enforcement Agents. As of this study's preparation date, 64 out of 145 active LEAs had completed the questionnaire. According to members of the Chamber, agents with no experience with cryptoassets were unlikely to complete the questionnaire.

Table 1. Experience of Enforcement Offices with Cryptoassets According to Length of Practice; author's own elaboration

Length of practice	No experience with enforcing cryptoassets	Cases with identified cryptoassets
10–19 years	24	4
20 years or more	23	2
5–9 years	10	0
Less than 5 years	1	0

Source: author's own elaboration.

More than 82% of respondents have been practising LEAs for more than 20 years, which ensures the high relevance and professional weight of their answers. As shown in Table 1, the results showed that 58 out of the 64 LEAs (over 90%) had never ordered or carried out any enforcement in which any cryptoassets were found. Of the remaining six LEAs who had directly

encountered cryptoasset enforcement in their practice, only one had dealt with multiple cases; the remaining five had dealt with only a few cases, and none had ever seized and subsequently monetised cryptoassets as part of these enforcement actions. The failures were primarily attributed to the assets being held with a foreign entity, the debtor not cooperating, or the lack of access to the account data.

It is also significant that 27 LEAs (more than 42% – see Figure 1) had encountered situations where the debtor had tried to conceal assets using cryptoassets, or where it was evident that the debtor owned cryptoassets but they could not be identified during the enforcement proceedings. The LEAs obtained this information through various means: from the creditor, from the debtor's bank account statements, or directly from the debtor, either through confirmation or through information shared on social media.

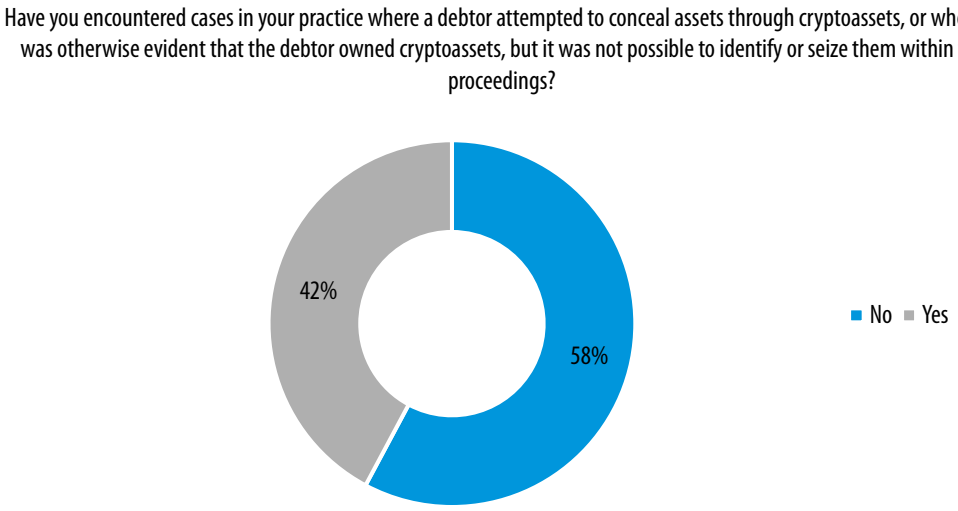

Figure 1. Cases Involving Debtors' Attempts to Conceal Assets via Cryptoassets
Source: author's own elaboration.

A total of 45 LEAs consider the current legal regulation to be entirely insufficient for the effective enforcement of enforcement title against cryptoassets. The remaining LEAs did not comment on the matter. The reasons for deeming the legal regulation to be insufficient are repeated and consist mainly of four key issues. First, there is the absence of specific legal regulations for the enforcement of cryptoassets. Second, there is a lack of effective tools for identifying and effectively sanctioning cryptoassets. Third, the partial anonymity of cryptocurrency wallets and the frequent use of foreign entities to purchase cryptoassets, which debtors then store them in, pose a challenge. Given these findings, more than 93% of LEAs expressed the need to introduce training, methodological support, or legislative changes in sanctioning digital assets in enforcement proceedings, as shown in Figure 2.

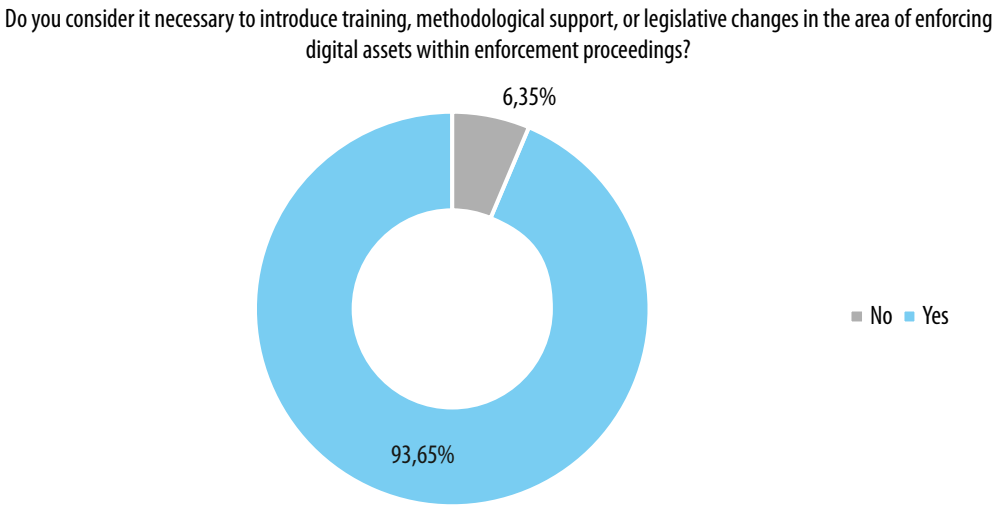

Figure 2. Perceived Need for Support and Legal Reforms in the Enforcement of Digital Assets
Source: author's own elaboration.

Insolvency Proceedings and Cryptoassets

In the Czech legal system, insolvency proceedings constitute a distinct legal process designed to satisfy creditors' claims while simultaneously protecting the insolvent debtor. In simplified terms, insolvency proceedings share objectives with enforcement proceedings namely, the identification, monetisation, and distribution of the debtor's assets among creditors although they differ in their procedural mechanisms. All the problematic aspects identified in connection with cryptoassets in enforcement proceedings are equally present in insolvency proceedings. The principal distinction lies in the position and authority of the insolvency administrator. In certain instances, the administrator is authorised to act on behalf of the debtor, allowing them to directly contact cryptocurrency exchanges, which are then obliged to cooperate (though this obligation applies primarily to domestic exchanges, not foreign entities). The insolvency administrator is further empowered to dispose of property freely and is not limited solely to auctions, as is the case in enforcement. This flexibility represents a considerable procedural advantage. Moreover, where the debtor fails to cooperate, for example, by withholding access to data to a crypto wallet or concealing the existence of assets, such conduct may lead to the failure of the insolvency proceedings, including the loss of eligibility for debt relief under Czech law. Given the substantial benefits of debt relief, the risk of forfeiting this option generally incentivises debtor cooperation.

In essence, however, all the substantive and procedural difficulties associated with cryptoassets in enforcement particularly issues of identification, access, and valuation also persist in insolvency proceedings.

Conclusion

This study has demonstrated that the enforcement of cryptoassets in the Czech Republic presents challenges of far greater complexity than those encountered in traditional enforcement proceedings. While enforcement against bank accounts or real estate operates within a clearly defined and predictable legal framework, cryptoassets continue to exist in a substantial legal and procedural vacuum. Their anonymity, technological opacity, decentralised structure, cross-border dimension, and the absence of a central authority collectively make debt recovery markedly more costly, time-consuming, and uncertain.

Although the Czech Civil Code recognises cryptoassets as intangible movable property, their practical enforcement is impeded by persistent ambiguities concerning the identification and location of digital wallets, the inability to compel debtors to disclose access credentials such as PIN codes or seeds, and the absence of standardised methods for valuation or transfer, particularly when assets are held on foreign exchanges.

Empirical evidence gathered from LEAs confirms that the issue is increasingly relevant in practice. Nonetheless, enforcement agents still lack the technical infrastructure and clear procedural methodology necessary for effective asset identification, seizure, and monetisation. Assets stored on foreign exchanges remain largely beyond the reach of domestic enforcement authorities, which are dependent on the voluntary cooperation of entities not subject to Czech jurisdiction. Likewise, the absence of a uniform valuation framework exacerbates uncertainty for both creditors and debtors.

Although some cryptoassets have already been monetised in public auctions, such procedures remain experimental and carry substantial risks arising from market volatility, settlement delays, and variable transaction fees. To minimise these risks, it is essential to establish rules that ensure fair valuation and procedural stability within the existing enforcement framework.

A sustained dialogue among legislators, legal scholars, practitioners, and technology experts is, therefore, crucial to developing procedures that reflect the technological realities of digital assets while safeguarding the legitimate interests of all parties. Without legislative intervention and institutional reform, cryptoassets will continue to represent an elusive and disproportionately costly form of property from which creditors cannot effectively satisfy their claims.

This gap in enforceability further confirms the broader risks identified in the literature on state sovereignty. The practical impossibility of securing assets held in private hardware wallets or on foreign exchanges effectively creates a safe haven for illicit financial flows. The Czech case thus illustrates a global paradox: while regulatory frameworks such as MiCA seek to standardise the market and establish harmonised rules for providers of services related to cryptoassets, the state's actual coercive authority remains limited not only by physical and technological barriers which in the digital sphere significantly weaken the state monopoly on the legitimate use of force but also by legal obstacles stemming from the absence of international cooperation among competent authorities. As a result, individuals may avoid state sanctions simply by shifting jurisdiction.

A functional legal framework must enhance cooperation with domestic and foreign crypto-exchange operators, particularly by obligating them to provide enforcement agents with verified data on account holders, balances, and transactions. Furthermore, it is necessary to develop dedicated enforcement instruments allowing for the freezing or blocking of digital wallets pursuant to an enforcement order, as well as to standardise valuation methods capable of reflecting extreme price fluctuations.

Implementing these measures would not only align legal practice with the technological evolution of financial markets but also enhance legal certainty for creditors while respecting the digital privacy of debtors. Ultimately, only the coordinated development of legislation, technical tools, and enforcement practice can transform cryptoassets from an inaccessible reservoir of value into an integral and enforceable component of modern legal systems both in the Czech Republic and across the EU.

The research was supported by the Czech Science Foundation Grant No. 24–12864S, titled 'Crypto Assets as a Threat to the Sovereign'.

References

Act No. 99/1963 Coll., Code of Civil Procedure, https://www.zakonyprolidi.cz/translation/cs/1963-99?langid=1033 (accessed: 9.05.2025).

Act No. 120/2001 Coll., Act on Bailiffs and Enforcement Activity (Enforcement Code) and on Amendments to Other Acts, https://www.zakonyprolidi.cz/translation/cs/2001-120?langid=1033 (accessed: 9.05.2025).

Act No. 253/2008 Coll., Act on Certain Measures against the Legalization of Proceeds of Crime and Terrorist Financing, https://www.zakonyprolidi.cz/translation/cs/2008-253?langid=1033 (accessed: 9.05.2025).

Act No. 89/2012 Coll., Civil Code, https://www.zakonyprolidi.cz/translation/cs/2012-89?langid=1033 (accessed: 9.05.2025).

Act No. 286/2021 Coll., Act amending Act No. 99/1963 Coll., the Code of Civil Procedure, as amended, Act No. 120/2001 Coll., on licenced enforcement agents and enforcement activities (the Code of Enforcement) and on amendments to other acts, as amended, and some other acts, https://www.zakonyprolidi.cz/cs/2021-286 (accessed: 9.05.2025).

Act of 17 November 1964 – Code of Civil Procedure, as amended, https://eli.gov.pl/api/acts/DU/1964/297/text/O/D19640297.pdf (accessed: 9.05.2025).

Cardao-Pito, T. (2025), *Can cryptocurrency exchanges threaten sovereign states? Lessons and hypotheses from the Binance case*, "Journal of Financial Crime", 32 (5), pp. 1030–1040, https://doi.org/10.1108/JFC-10-2024-0336

Český statistický úřad (2025), *Průměrné mzdy – 4. čtvrtletí 2024*, https://csu.gov.cz/rychle-informace/prumerne-mzdy-4-ctvrtleti-2024 (accessed: 11.04.2025).

Daňhel, R. (2025), *Aukční vyhláška: Č. j.: MSP-76/2025-OIM-SML2/1*, https://www.nabidkamajetku.gov.cz/api/Property/Attachment/2be8044b-02f7-421c-8dcf-b60ace2a25ef (accessed: 9.05.2025).

Dupuis, D., Gleason, K. (2020), *Money laundering with cryptocurrency: open doors and the regulatory dialectic*, "Journal of Financial Crime", 28 (1), pp. 60–74, https://doi.org/10.1108/JFC-06-2020-0113

Dvořák, J., Švestka, J., Zuklínová, M. (2016), *Občanské právo hmotné. 2. aktualizované a doplněné vydání*, Wolters Kluwer, Prague.

Erp, S. (2022), *Komorní listy: Digitální aktiva… „fantomový dlužník"*, "Exekutorská komora České republiky", 12 (2), pp. 22–25.

Exekutorská komora České republiky (2025), *Počet fyzických osob v exekuci a další podrobnosti*, https://statistiky.ekcr.info/otevrena-data (accessed: 4.11.2025).

Ferreira, A., Sandner, P. (2021), *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*, "Computer Law & Security Review", 43, 105632, https://doi.org/10.1016/j.clsr.2021.105632

Heyman, C.E.(R.) (2023), *A red flag checklist for cryptocurrency Ponzi schemes*, "Journal of Financial Crime", 31 (3), pp. 711–747, https://doi.org/10.1108/JFC-05-2023-0118

Hrabčák, L., Štrkolec, M. (2024), *EU Regulation of the Crypto-Assets Market*, "Białostockie Studia Prawnicze", 29 (1), pp. 27–45, https://doi.org/10.15290/bsp.2024.29.01.02

Institut prevence a řešení předlužení (2025a), *Exekuce*, https://www.institut-predluzeni.cz/mapy-a-statistiky/exekuce/ (accessed: 11.04.2025).

Institut prevence a řešení předlužení (2025b), *Podíl osob v exekuci po krajích (Q4 2024)*, https://mapazadluzeni.cz/?g=kraj&v1=podil_osob_v_exekuci&v1p=2024-Q4 (accessed: 13.04.2025).

Institut prevence a řešení předlužení (2025c), *Podíl osob v exekuci po krajích (2022, Q4 2023, Q4 2024 a Q1 2025)*, https://mapazadluzeni.cz/?g=kraj&v1=podil_osob_v_exekuci&v1p=2022&v1p=2023-Q4&v1p=2024-Q4&v1p=2025-Q1&vis=table (accessed: 15.04.2025).

Institut prevence a řešení předlužení (2025d), *Podíl osob s více exekucemi po krajích (2022, Q4 2023, Q4 2024 a Q1 2025)*, https://mapazadluzeni.cz/?g=kraj&v1=podil_exekvovanych_s_2_a_vice_exekucemi&v1p=2022&v1p=2023-Q4&v1p=2024-Q4&v1p=2025-Q1&vis=table (accessed: 10.04.2025).

Irwin, A.S.M., Milad, G. (2016), *The use of crypto-currencies in funding violent jihad*, "Journal of Money Laundering Control", 19 (4), pp. 407–425, https://doi.org/10.1108/JMLC-01-2016-0003

Jones, H. (2023), *EU urges others to copy its rules for cryptoassets*, https://www.reuters.com/technology/eu-urges-others-copy-its-rules-cryptoassets-2023-04-19/ (accessed: 28.10.2025).

Judgment of the Supreme Administrative Court of 6 March 2018, file reference II FSK 488/16, https://www.inforlex.pl/dok/tresc,NSA.2018.001.100009851,Wyrok-NSA-z-dnia-6-marca-2018-r-sygn-II-FSK-488-16.html (accessed: 28.10.2025).

Kabra, S., Gori, S. (2023), *Drug trafficking on cryptomarkets and the role of organized crime groups*, "Journal of Economic Criminology", 2, 100026, https://doi.org/10.1016/j.jeconc.2023.100026

Kaliský, B. (2018), *Bitcoin a ti* druzí: nepostradatelný *průvodce světem kryptoměn*, IFP Publishing, Prague.

Kohajda, M., Moravec, J. (2021), *Legal Issues of Stablecoins*, "Daně a finance", 28 (1–4), pp. 93–98, https://www.researchgate.net/publication/357428892_Legal_Issues_of_Stablecoins (accessed: 19.06.2025).

Kozieł, M. (2025), *New Regulation of Crypto-Assets in the European Union as an Opportunity and a Threat for Entrepreneurs*, [in:] S. Kot, B. Khalid, A. ul Haque (eds.), *New Challenges of the Global Economy for Business Management*, Springer Proceedings in Business and Economics, Singapore, pp. 791–805, https://doi.org/10.1007/978-981-96-4116-1_50

Mackenzie, S. (2024), *Crypto collapse: the cult of personality and the normalisation of fraud in FTX and Celsius*, "Journal of Financial Crime", 32 (2), pp. 288–303, https://doi.org/10.1108/JFC-01-2024-0054

Maume, P. (2023), *The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification, or First Step of Many, or Both?*, "European Company and Financial Law Review", 20 (2), pp. 243–275, https://doi.org/10.1515/ecfr-2023-0014

Morton, T. (2020), *The Future of Cryptocurrency: An Unregulated Instrument in an The Future of Cryptocurrency: An Unregulated*, "International Journal of Social Sciences", 4 (1), pp. 555–570, https://lawecommons.luc.edu/lucilr/vol16/iss1/8 (accessed: 19.06.2025).

Nabilou, H. (2019), *How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency*, "International Journal of Law and Information Technology", 27 (3), pp. 266–291, https://doi.org/10.1093/ijlit/eaz008

Ocampo, D.G., Branzoli, N., Cusmano, L. (2023), *Crypto, tokens and DeFi: navigating the regulatory landscape*, https://www.bis.org/fsi/publ/insights49.htm (accessed: 17.10.2025).

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng (accessed: 17.10.2025).

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. OJ L 150, 9 June 2023, https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng (accessed: 17.10.2025).

Takei, Y., Shudo, K. (2024), *Pragmatic Analysis of Key Management for Cryptocurrency Custodians*, [in:] *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 27–31 May, Ireland, pp. 747–765, https://doi.org/10.1109/ICBC59979.2024.10634356

Tiwari, M., Lupton, C., Bernot, A., Halteh, K. (2024), *The cryptocurrency conundrum: the emerging role of digital currencies in geopolitical conflicts*, "Journal of Financial Crime", 31 (6), pp. 1622–1634, https://doi.org/10.1108/JFC-12-2023-0306

Van der Linden, T., Shirazi, T. (2023), *Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?*, "Financial Innovation", 9 (1), https://doi.org/10.1186/s40854-022-00432-8

Wronka, C. (2021a), *Digital currencies and economic sanctions: the increasing risk of sanction evasion*, "Journal of Financial Crime", 29 (4), pp. 1269–1282, https://doi.org/10.1108/JFC-07-2021-0158

Wronka, C. (2021b), *Financial crime in the decentralized finance ecosystem: new challenges for compliance*, "Journal of Financial Crime", 30 (1), pp. 97–113, https://doi.org/10.1108/JFC-09-2021-0218

Xu, X., Weber, I., Staples, M. (2019), *Architecture for Blockchain Applications*, Springer, Cham, https://doi.org/10.1007/978-3-030-03035-3

Zetzsche, D.A., Arner, D.W., Buckley, R.P. (2020), *Decentralized Finance*, "Journal of Financial Regulation", 6 (2), pp. 172–203, https://doi.org/10.1093/jfr/fjaa010

Kryptoaktywa jako zagrożenie dla suwerenności państwa w obszarze egzekucji i niewypłacalności

Kryptoaktywa, jako nowatorska forma technologii finansowej, stanowią wyzwanie dla tradycyjnych ram prawnych, zwłaszcza ze względu na swój zdecentralizowany charakter oraz specyficzny sposób przechowywania i transferu. Ich pojawienie się wymaga ponownego przeanalizowania zasad regulacyjnych i mechanizmów ochrony praw uczestników rynku kryptoaktywów w środowisku, w którym decentralizacja oznacza brak scentralizowanej kontroli. W niniejszym artykule omówiono kryptoaktywa jako potencjalne zagrożenie

dla suwerenności państwa w obszarach egzekucji i niewypłacalności. Przeanalizowano wyzwania legislacyjne wynikające z rosnącej popularności kryptoaktywów oraz oceniono możliwość zastosowania tradycyjnych instrumentów prawa egzekucyjnego w kontekście tych nowych technologii.
W opracowaniu przedstawiono również wyniki badań empirycznych dotyczących czeskiego środowiska prawnego w szerszym kontekście teoretycznym, dotyczącym przestępstw finansowych i erozji władzy państwowej spowodowanej zdecentralizowanymi systemami finansowymi działającymi w różnych jurysdykcjach krajowych. Szczególną uwagę poświęcono technicznym cechom kryptoaktywów, ich klasyfikacji prawnej oraz praktycznym przeszkodom napotykanym w postępowaniach egzekucyjnych i upadłościowych, zwłaszcza w sytuacjach, gdy dłużnicy odmawiają lub nie są w stanie zapewnić dostępu do swoich aktywów cyfrowych.
Analiza uwzględnia również dostępne statystyki dotyczące postępowań egzekucyjnych i poddaje ocenie czeskie ramy prawne funkcjonowania kryptoaktywów, koncentrując się na ich wpływie na skuteczność procesów egzekucyjnych i upadłościowych. W badaniach wykorzystano zarówno metody pierwotne, jak i wtórne, w tym analizę prawną i techniczną, modelowanie rzeczywistych scenariuszy oraz badanie odpowiednich instrumentów prawnych.

Słowa kluczowe: Czechy, kryptowaluta, postępowanie egzekucyjne, niewypłacalność, ramy prawne