№
4

Cryptocrimes

To what extent are cryptocrimes addressed by the legal frameworks of the European Union and the Netherlands?

Laurie Ritzen

MAASTRICHT LAW SERIES

Cryptocrimes

Cryptocrimes

To what extent are cryptocrimes addressed by the legal frameworks of the European Union and the Netherlands?

Laurie Ritzen

WJS UITGEVERS

Omslagontwerp: Nick van Silfhout
Opmaak binnenwerk: Crius Group, Hulshout

ISBN 978-94-93458-04-8
NUR 820

wjs-uitgevers.nl

Acknowledgements

It has been a privilege to carry out this PhD and I owe a great debt of gratitude to many who have supported me along the way.

I am particularly grateful to my supervisors for their unwavering support throughout this journey. Tijs, your sharp legal analyses and our many meaningful conversations have not only challenged but also inspired me. Matthijs, your clear insights, our sparring sessions and the way you always highlighted the practical consequences of my ideas have been of tremendous value. More than that, both of you have offered reassurance precisely when it was most needed. Your trust in me – especially at those times when I struggled to find that trust in myself – has been truly decisive. Your reassurance during the more difficult moments has meant more than words can say.

I would also like to thank François Kristen, Jan-Jaap Oerlemans, Jannemieke Ouwerkerk and Elies van Sliedregt for reading and approving the manuscript. I truly appreciate your valuable feedback and will certainly carry your insights with me into the future.

Two people deserve particular mention for shaping the course of my academic path even before this PhD began. Joep Simmelink, when I was his student-assistant, initiated the contact with Tilburg that ultimately allowed me to embark on this journey. André Klip played a decisive role in my first steps as a researcher. I remain profoundly grateful to both of you for setting me on this path.

I also wish to extend my appreciation to all colleagues with whom I have had the pleasure of working over the years in the departments of Tilburg University and Maastricht University. In particular, I want to thank Sjors Ligthart and Janneke van der Ham for being my paranymphs. Beyond being exceptionally clever minds who have consistently challenged me, they are also a pleasure to work with and to have by my side. I am especially grateful for their patience with my endless complaints – as it turns out, good humour and a sense of perspective are just as important as sharp debate.

Of course, many colleagues have made this journey memorable, but a few deserve special mention. Rachel, I still remember us at our first PhD course – both blissfully unaware of what we had signed up for. Now here we are, somehow still standing at the finish line. I could not have asked for better company along the way. Stijn, thank you for your unwavering optimism throughout. I look forward to where our intersecting research interests may take us next. Richi, thank you for all the laughter and serious conversations along the way. I deeply appreciate your wise words when times were tough. And remember – there is still time for us to become a train conductor should academia ever lose its charm. Joyce, from being the second supervisor of your thesis to becoming colleagues and friends, it has been quite a journey. From laughter to the odd tear, those

digital coffee breaks and dinners during lockdowns remain some of my favourite memories of this whole period. Joeri, although our paths at Tilburg only just overlapped, I'm glad we had the chance to work together during my internship at the Dutch Supreme Court. I truly appreciate your support and advice during these final stages.

I also want to extend my sincerest thanks to the Department of Criminal Law and Criminology at Maastricht University for graciously allowing me to complete this dissertation. Among all the wonderful colleagues in Maastricht, there are a few to whom I owe special thanks. Christina, thank you for your wise counsel and sharp perspectives. They have guided me more often than you probably realise. Johannes, thanks for the mental back-up in those final stages; I suspect my nerves would have been in far worse shape otherwise. Sophie, your energy and passion at the start of your PhD have been a delight to see, particularly while I was perfecting the art of complaining my way to the finish line. Peggy, thank you for your thoughtful feedback and excellent company, even when we both had much on our 'plate'. Suzan, collaborating with you on new projects has been a real pleasure. I am grateful for the opportunities and guidance you have offered – and for the good humour that has come with it.

And last, but by no means least, I want to thank Russell. You have had the dubious honour of living through every high and low by my side and experienced far more of this process than anyone could reasonably be expected to endure. Your support has meant everything. I want to thank you for always being there for me, never holding me back but standing beside me, every step of the way – even as I was powered by caffeine, nicotine and the unhinged determination of a sleep deprived goblin whispering 'this is fine' while everything burned. And of course, thanks to Bailey, Peanut, Mellow and Moon, whose unwavering cheer (and complete disregard for personal space) helped keep me grounded. Even though not all of them made it to the finish line with us, they were very much part of this journey. I could not have picked a set of clumsier, more drool-intensive therapists if I had tried.

Heerlen,
3 July 2025

Table of contents

List of abbreviations

AWR	*Algemene wet inzake rijksbelastingen* (Dutch State Taxes Act)
CFSP	Common Foreign and Security Policy
CJEU	Court of Justice of the European Union
DAO	Decentralised Autonomous Organisation
DCC	Dutch Criminal Code
EBA	European Bank Authority
ECJ	European Court of Justice
ECHR	European Convention for the protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
ESMA	European Securities and Markets Authority
FATF	Financial Action Task Force
ICO	Initial Coin Offering
IPO	Initial Public Offering
IRS	Internal Revenue Service
IW	*Invorderingswet 1990* (Collection of State Taxes Act 1990)
NCA	National Competent Authority
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
The DAO	The Decentralised Autonomous Organization
WED	*Wet op de economische delicten* (Law on Economic Offences)
Wft	*Wet op het financieel toezicht* (Financial Supervision Act)
Wwft	*Wet ter voorkoming van witwassen en financieren van terrorisme* (Money Laundering and Terrorist Financing (Prevention) Act
SW	*Sanctiewet 1977* (Dutch Sanctions Act 1977)

Part I

INTRODUCTORY CONSIDERATIONS

1. Introduction

1. Background

On 28 March 2019, I received an email in which the sender claimed to have unlawful access to my smartphone, asserting possession of an indecent video of me.[1] The email demanded that I pay a 'donation' in bitcoin[2] or the video would be sent to my entire contact list. An old password of mine was included in the email as 'proof' of the individual's access to my phone. It appears that some recipients of similar messages were convinced of their credibility, as evidenced by payments made.[3] The sender, however, was most likely unaware of the futility of their efforts in my case given my ongoing research on crypto-assets and prior knowledge of such scams.

Blackmail is just one of many improper uses of crypto-assets observed today. In this dissertation, the term 'crypto-assets' is used as an umbrella term for various types of cryptocurrencies and tokens. The media frequently report on questionable activities in this realm, with (successful) criminal prosecutions for crypto-assets related behaviour visibly increasing in the Netherlands since 2017.[4] The tendency to use crypto-assets for malicious activities can be traced to their unique features, such as (pseudo-)anonymity, irreversibility, a decentralised set-up, and the usage of cryptography. These assets facilitate serious crimes, and there is considerable abusive behaviour in the issuance and trading of these assets. For example, crypto-assets are extensively used as a 'currency' on the dark web.[5] In addition, their issuance and trading are often associated with fraud, insider trading and market manipulation.[6] However, the extent to which such unwanted behaviour is regulated remains unclear due to a lack of comprehensive research on malicious activities related to crypto-assets from a criminal law perspective.

These issues have grown more prominent as the crypto-community has expanded.[7] As the usage of crypto-assets – and therefore their issuance and trading on related markets –

---

1 Annex IA.

2 The accepted practice within the crypto-community is to use Bitcoin (with an uppercase "B") when referring to the payment network, its protocol or its software; while bitcoin (with a lowercase "b") denotes a unit of the currency. The plural form, bitcoins, is typically used for numerically quantified amounts (e.g. 15 bitcoins).

3 Digital Shadows 2018, p. 5; D. Verlaan (*RTL Nieuws*) 2018.

4 According to the Dutch database www.rechtspraak.nl (using the keyword 'bitcoin').

5 Barysevich & Solad 2018, p. 4-6.

6 J. Titcomb (*The Telegraph*) 2017.

7 For example, in 2022 the total market capitalisation of crypto-assets varied between approximately $ 800 billion and 2.2 trillion. See CoinMarketCap, 'Global Charts', https://coinmarketcap.com/charts/.

becomes (more) mainstream, unwanted behaviour may occur on a larger scale, posing greater threats to society and even to the stability of the financial systems. Hence, the use of crypto-assets for malicious activities, driven by their unique features and uncertainty surrounding the legal status of such behaviour, presents a significant societal issue.

A wide variety of illicit behaviour surrounding crypto-assets is discussed in this dissertation. These various forms of harmful behaviour can be divided into two general categories

i) Abusive behaviour surrounding the issuance and trading of crypto-assets, and
ii) Crimes facilitated by the usage of crypto-assets.

I refer to them together as 'crypto-asset related crimes and abuse', or 'cryptocrimes' for short.

The first category includes abusive behaviour related to the issuance and trading of crypto-assets, such as fraud and market abuse. A key characteristic of these cryptocrimes is that the 'place', the *locus delicti*, of the violations has shifted from traditional, non-crypto markets to the (ostensibly) unregulated area of crypto-assets.

The second category consists of crimes that are facilitated by the use of crypto-assets, such as money laundering and blackmail. The distinctive element for this group is the change in the *modus operandi* of the crime. While the outcomes are similar, offenders use crypto-assets instead of traditional objects, such as cash or electronic money.

Due to the unique traits of crypto-assets and the current (perceived) lack of clarity regarding the applicable legal framework, debates persist about the shift of criminal behaviour toward cryptocrimes.[8] Legislative gaps, or 'grey areas', and favourable characteristics create convenient circumstances for (first-time) offenders with an opportunistic mindset. Hence, this dissertation aspires to clarify the applicable legal framework(s) and, if considered to be necessary, propose reforms to help to prevent and mitigate the displacement of crimes toward the realm of crypto-assets. These insights may lead to improved protection for consumers and financial institutions. In addition, (further) regulation will increase the (perceived) integrity of crypto-asset markets, which are occasionally referred to as the 'Wild West' of the financial industry.[9]

Amid ongoing debates about crypto-assets, particularly bitcoin, this study's findings can significantly contribute to the international theoretical discussion among scholars, authorities and lawmakers regarding crypto-asset regulation and the countering of cryptocrimes. In addition, with regard to recommendations for reform, the dissertation aims to support the establishment of a legal framework for the issuance, trading and use of crypto-assets.

2. Central research question

Although there is ongoing debate concerning the regulation of crypto-assets, the consensus is that these assets are here to stay and legislatures should focus on mitigating their negative

8 FATF 2014, p. 9-10; Houben & Snyers 2018, p. 9; Kethineni & Cao 2019, p. 5-6; Keatinge et al. 2018, p. 9-10.

9 E.g. Treasury Committee 2018, p. 33 and 43; Chavez-Dreyfuss (*Reuters*) 2018 and Robinson 2018.

effects, such as regulating criminal activities.[10] The growth of the crypto-community and the accompanying risks have compelled lawmakers and (financial) authorities to take crypto-assets seriously, evaluating measures to regulate them in order to counter cryptocrimes. The principal research question raised by the societal problem of crypto-asset related crimes and abuse is thus as follows:

Would additional legislation on a European and/or Dutch level be necessary to effectively counter cryptocrimes, and, if so, how should cryptocrimes be regulated?

This central research question focusses on a Dutch and European context[11] and is predominantly normative in nature. This normative aspect is divided into two components: an evaluative component and a reform oriented component. Based on the existing body of knowledge, it appears that certain cryptocrimes are insufficiently regulated.[12]

Despite an increase in unwanted behaviour, comprehensive research, and thus knowledge, on these activities and corresponding legal frameworks remains scarce. Previous studies have often focussed on specific forms of cryptocrimes, and, in some cases, it remains unclear on which criteria assessments were based.[13] Therefore, it is essential to extensively analyse the observed types of unwanted behaviour. This fundamental review provides detailed insight into existing issues and is a prerequisite for the part aimed at revision. Based on prior contributions to the field, the working proposition is that additional legislation at both the European and Dutch levels is necessary to counter crypto-asset related crimes and abuse.

The central research question focusses on cryptocrimes, necessitating a clear definition of behaviour that qualifies as such. The concept of a cryptocrime is shaped by the notion of a 'criminal offence' within the meaning of Article 7 of the European Convention for the protection of Human Rights and Fundamental Freedoms (ECHR).[14] While a State's classification of behaviour in its legal system ascertains if there is a criminal offence,[15] this factor is less significant than the other two factors, namely the nature and objective of the

---

10 E.g. the head of the U.S. Treasury Department stated that his number-one focus on crypto-assets is to make sure that they are not used for illicit activities (See: S. Kim & S. Robinson, (*Reuters*) 2018). In addition, the chairmen of the U.S. Securities and Exchange Commission (SEC) and the U.S. Commodity Futures Trading Commission (CFTC) indicated that they would focus on protecting consumers against initial coin offering fraud and unregulated exchanges (See: J. Clayton (*SEC)*; C. Giancarlo (*Cftf*) 2018). This is also demonstrated by Directive 2018/843 (AMLD5), specifically designed to include crypto-assets.

11 See § 5 of this chapter for a justification on the scope of this dissertation.

12 E.g. AFM (*AFM*) 2017 and ESMA 2019, p. 29-30.

13 The cryptocrime of money laundering has been a primary focus of previous research. E.g. Oerlemans et al. 2016; Vandezande 2018a; Warnaars 2019.

14 In the absence of a concrete definition of criminal law by the ECJ, reference is made to the definition provided by the ECtHR. See ECtHR judgement of 8 June 1976, *Engel and Others*, Series A No. 22; ECtHR judgement of 21 February 1984, *Öztürk*, Series A No. 73; CJEU judgement of 5 June 2012, *Łukasz Marcin Bonda*, Case C-489/10; CJEU judgement of 26 February 2013, *Åklagaren v. Hans Åkerberg Fransson*, Case C-617/10.

15 The ECtHR interprets 'criminal offence' under Article 7 ECHR in accordance with the criteria set for 'criminal charge' in Article 6 ECHR. See ECtHR judgement of 17 May 2016, *Société Oxygène Plus v. France,* par. 43; ECtHR judgement of 4 October 2016, *Žaja v. Croatia,* par. 86.

offence and the nature and severity of the penalty.[16] Therefore, the behaviours examined in this dissertation may have a legal basis in criminal law and/or punitive administrative law, as defined by Article 7 of the ECHR. Illicit activities related to the issuance and trading of crypto-assets are addressed under both punitive administrative and criminal law frameworks. The activities in which crypto-assets are utilised to facilitate crimes have, in contrast, a basis predominantly in criminal legislation in the Dutch legal system.

Given the current lack of comprehensive knowledge on the types of cryptocrimes, this study focusses exclusively on completed cryptocrimes. Inchoate offences, such as attempted or preparatory acts, fall outside the scope of this dissertation and are addressed only marginally, where specific challenges for cryptocrimes are anticipated. In addition, the forms of participation will also be excluded. Further research on these topics is recommended.

The overarching goal of this dissertation is to clarify and, if considered necessary, tighten the legal framework to counter crypto-asset related crimes and abuse. This aim presumes that stricter regulation will reduce criminal activity, which is intertwined with a view of human beings as rational, calculating individuals. While this view has been criticised,[17] it forms the underlying premise of criminal and/or administrative regulations on the Dutch and European levels.[18]

The central research question can be divided into the following four sub-questions.

1. *What types of cryptocrimes can be identified in relation to the issuance, trading and usage of crypto-assets?*

This dissertation begins with an assessment of archetypical forms of cryptocrimes. This overview is not limited to crimes emerging in the Netherlands or the European Union. Instead, it incorporates information on the types of actual cryptocrimes from around the world to ensure general relevance for this section of the dissertation. The analysis is primarily descriptive and thus various sources are used, including reports from lawmakers, authorities and international organisations on the status of cryptocrimes in addition to news reports, case law and scholarly literature on the topic of cryptocrimes.

2. *What are the relevant existing European and Dutch legal frameworks for the identified cryptocrimes?*

The study continues with an assessment of European and Dutch legislation, examining their relevance to the cryptocrimes identified under sub-question 1. Relevance is measured by resemblances between the factual behaviour that underlies a certain type of cryptocrime and already regulated unwanted behaviour. For example, the practical steps required to

16 ECtHR judgement of 8 June 1976, *Engel and Others*, Series A No. 22, par. 82; ECtHR judgement of 21 February 1984, *Öztürk*, Series A No. 73, par. 50.

17 See Ulen 1999, p. 800-806; Korobkin & Ulen 2000, p. 1066-1070; Hodgson 2012.

18 Recommendations for regulations (*Aanwijzingen voor de regelgeving*) *Stcrt.* 2017, 69426, rec. 2.2.; Klip 2021, p. 291-292; Council conclusions on model provisions, guiding the Council's criminal law deliberations, 30 November 2009, p. 2; European Parliament resolution of 22 May 2012 on an EU approach to criminal law, par. 3.

commit insider trading – that is, having privileged information and using it for one's own benefit – can be separated from the law that prohibits it. Are these steps alike in a market that is within the scope of the Market Abuse Regulation,[19] such as financial instruments traded on a multilateral trading facility,[20] and the crypto-asset market? If so, the Market Abuse Regulation would be considered relevant to this type of cryptocrime.

To conduct this assessment, legal sources are examined. The selected legislation, applicable case law and relevant scholarly literature are subjected to an in-depth analysis to ascertain the applicable legal regime.

3. Are the current legal frameworks sufficient to effectively counter cryptocrimes?

The third sub-question introduces the first normative assessment.[21] Once the applicable legal regime has been identified, its sufficiency and effectiveness in regulating the specific cryptocrime is evaluated. As noted, it seems evident that certain behaviour is currently insufficiently regulated. However, this still raises several key questions: What are the precise issues with the existing legal framework? Do they concern the scope of the framework? Is the framework itself not suitable for addressing cryptocrimes? These and other questions are explored using the evaluative normative framework.

4. To the extent that cryptocrimes are not covered by European and Dutch legal frameworks, should the behaviour be regulated and, if so, how?

The second normative part of the study examines whether cryptocrimes that are currently insufficiently and/or ineffectively regulated at the European Union and/or Dutch level require amendments to the legal frameworks. This normative framework is desiderative in nature, evaluating how we desire the law to be. Its foundation lies in the principle of crypto and non-crypto equivalence, an analogue to the concept of online and offline equivalence. Building on the relevant legal frameworks identified under sub-questions 1 and 2, the study assesses whether and how the cryptocrime(s) are, or should be, regulated. The concept of crypto and non-crypto equivalence, along with the desiderative framework, are explored in greater detail in § 4.2.2 of this chapter.

The methods employed to answer the sub-questions vary and are outlined in § 4 of this chapter.

3. Structure of the book

This book is organised into four parts, each of which is introduced in this section to provide an overview of the dissertation's structure.

---

19 Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.

20 Article 2, paragraph 1 sub b, Regulation 596/2014.

21 The criteria of the first normative framework are explained in § 4.2.1 of this chapter.

Part I: Introductory considerations
The aim of Part I is to provide readers with fundamental background information on the key elements of this dissertation (Chapter 1) and an introduction to the basics of crypto-assets (Chapter 2). Accordingly, no specific research question(s) are addressed here. As Jennifer Shasky Calvery, then Director of the Financial Crimes Enforcement Network, signalled during a 2013 conference, 'While probably most of today's audience understands what these emerging payments systems are and how they work, many line analysts, investigators, and prosecutors in law enforcement may not.'[22] This observation remains relevant as the need for accurate and accessible knowledge persists. This is partly due to an absence of literature that deals with all aspects of crypto-assets in a comprehensible matter for anyone involved with cryptocrimes while still doing justice to the underlying techniques of these assets. While some work does meet this standard, it often fails to explicitly connect the unique aspects of crypto-assets to their implications for the criminal and administrative legal system. Furthermore, crypto-assets have not escaped the pervasive issue of 'fake news', even within mainstream media.[23] For these reasons, an introductory chapter that deals with the fundamentals of crypto-assets from a legal perspective is indispensable to this dissertation. However, given the emphasis on fundamental aspects relevant to criminal and administrative law, the introduction in Chapter 2 is not exhaustive.

Part II: Abusive behaviour surrounding the issuance and trading of crypto-assets
The second part of this book delves into the various forms of crypto-asset related crime and abuse associated with the issuance and trading of these assets. Chapter 3 focusses on the crime of cryptojacking, while Chapter 4 examines fraud related to initial coin offerings. Chapter 5 addresses the different forms of market abuse. Each cryptocrime is evaluated using the framework established by the four previously discussed sub-questions.

Part III: Crimes facilitated by crypto-assets
Part III examines criminal activities facilitated by crypto-assets, which are divided into two categories. The first category consists of property-related crimes and abuses, discussed in Chapters 6 to 8. Chapter 6 addresses the unlawful obtainment of crypto-assets (crypto-theft), Chapter 7 focusses on how these assets are used in extortion and blackmail schemes, and Chapter 8 examines the crime of embezzlement.

The second category includes crimes of a subversive nature that have the potential to threaten society or financial stability. These are covered in Chapters 9 to 12, which explore money laundering (Chapter 9), financing terrorism (Chapter 10), tax offences (Chapter 11) and bypassing economic sanctions (Chapter 12). Both categories are thoroughly assessed using the four aforementioned sub-questions.

Part IV: Final remarks
The final part of this dissertation presents an overall conclusion and offers a reflective analysis of Parts II and III.

---

22 J.S. Calvery, (*National Cyber-Forensics Training Alliance*) 2013.
23 E.g. J. Rice, (*Crypto Briefing*) 2018; M. Cavicchioli (*The Cryptonomist*) 2018.

4. Research methods

4.1. Introduction

This dissertation adopts an interdisciplinary approach, bridging both legal and non-legal research domains. It integrates insights from diverse fields, including crypto-assets theory, regulatory theories, legal concepts of equivalence, and economic theories on financial markets. Using a mixed-methods approach, it combines descriptive, doctrinal and normative research methodologies to address the central research question. This section provides further elaboration on the normative frameworks underpinning this dissertation.

4.2. Normative frameworks

In § 2 of this chapter, I outlined the necessity of employing two distinct normative frameworks to answer the main research question. Each normative framework originates from a different starting point and, accordingly, applies its own criteria. The first framework is evaluative in nature (§ 4.2.1). It examines whether the existing European and Dutch legal frameworks are sufficient to effectively counter cryptocrimes. The second normative framework is desiderative in nature (§ 4.2.2). It evaluates how the law should be (modified) to comprehensively cover and counter crypto-asset related crimes and abuse. Through this framework, the gaps identified in the legal frameworks via the evaluative normative framework are analysed to ascertain whether additional legislation is necessary and desirable.

4.2.1. Evaluative normative framework

The evaluative normative framework is employed to evaluate whether an existing legal framework is applicable to the identified cryptocrimes and if it is sufficient and effective in countering them. This section outlines the criteria that form the basis of this assessment. The evaluation within this framework is structured around two key questions:

1. Does the identified legal framework impose a sufficient basis to establish criminal[24] liability?
2. Is the legal framework effective in application?

The first question is assessed based on elements derived from the legality principle, approaching the sufficiency of an existing legal framework from a legal perspective. If the assessment results are affirmative, the evaluation proceeds to the second question. However, if the legal framework is considered to be insufficient, the conclusion should be that the cryptocrime is momentarily not covered by legislation, rendering evaluation

[24] The term 'criminal' is used in accordance with the interpretation of 'criminal offence' (Article 7 ECHR) and 'criminal charge' (Article 6 ECHR). Consequently, its scope is broader than the national definition of criminal liability and also includes liability for certain administrative offences under Dutch law (see § 2 of this chapter).

of the second question futile. In such cases, the desiderative normative framework is applied as the next step (§ 4.2.2).

The second question covers the practical effectiveness of applying the current legal framework to a specific type of cryptocrime. This review considers not only the unique features of crypto-assets but also the side effects of application in a broader sense. In other words, it is reviewed whether there are discrepancies in the application of the legal framework to crypto-assets versus its application to non-crypto-related crime and abuse.

A more detailed clarification of the framework regarding sufficiency (§ 4.2.1.1) and effectivity (§ 4.2.1.2) is provided in the following sections. Given the close connection to existing legal frameworks, I also discuss the methods of interpretation employed in this dissertation (§ 4.2.1.3). Finally, I present a schematic overview of the evaluative normative framework in § 4.2.1.4.

4.2.1.1. A sufficient basis for criminal liability

The legality principle is enshrined in various legal provisions, including Article 49 of the Charter of Fundamental Rights of the European Union (Charter), Article 7 of the ECHR,[25] Article 16 of the Dutch Constitution, Article 1 of the Dutch Criminal Code (DCC), and Article 5:04 of the Dutch General Administrative Law Act.[26] Consequently, this principle is firmly established at both the Dutch and European levels and serves as a cornerstone of criminal and administrative legislation.[27] Each of the aforementioned articles encompass various norms directed at either the legislature or the judiciary.[28] The principle entails a normative feature whereby 'it defines what law is, in other words, it identifies the legitimate sources of criminal liability'.[29] While a comprehensive examination of all aspects of the legality principle lies beyond the scope of this dissertation, I focus on the elements most relevant to the evaluative normative framework: *lex scripta*, *lex certa* and *lex stricta*.[30] These elements are briefly outlined below, followed by an explanation of their implications for the normative evaluation.

The first element of the legality principle incorporated in the evaluative normative framework is commonly referred to as *lex scripta*. This norm requires that criminal liability

---

25 Article 7 ECHR constitutes a substantive view of the legality principle and the applicability is therefore not limited to the field of criminal law but depends on the evaluation of a 'criminal offence'. See Nan 2011, p. 142, 150. It is not immediately clear whether Article 49 Charter adopts a formal or substantive approach. Neither the text nor the case law of the Court of Justice of the European Union provides a definitive answer. Based on a systematic interpretation and in light of Article 6 TEU and Article 52, paragraph 3, Charter, it is assumed that Article 49 also encompasses a substantive approach to the application of the legality principle. See EU Council, *Explanations relating to the Charter of Fundamental Rights, Explanation on Article 49*, December 2007. Support for this view can also be found in the CJEU judgement of 8 September 2016, *Merck KGaA v. European Commission*, Case T-470/13, the Court of Justice of the European Union noted in par. 463: 'In addition, the scope of what is foreseeable depends to a considerable degree on the content of the text at issue, the field which it covers and the number and status of those to whom it is addressed'. This judgement indicates that the element of *lex certa* is not limited to the field of criminal law.

26 The interpretation of the legality principle for administrative law connects with Article 7 ECHR, Article 16 Dutch Constitution and Article 1 DCC. See *Kamerstukken II* 2003/04, 29702, 3, p. 85.

27 Klip 2021, p. 245; Peristeridou 2015, p. 33, 78; Kristen 2010, p. 641.

28 See Kooijmans 2023; Klip 2021, p. 245-257; Altena 2016; Peristeridou 2015.

29 Peristeridou 2015, p. 71.

30 Recommended readings: Nan 2011, Peristeridou 2015, Altena 2016, Timmerman 2018, Kooijmans 2023.

must have a basis in written law.[31] From the perspective of legality, Charter Article 49 encompasses a broad meaning of the term 'law', which includes legislation at the level of the European Union.[32] However, the obligations of Member States to implement such legislation cannot be disregarded. Even if it aligns with the legality principle that criminal liability is based on European Union law, it could be contradictory to the obligations of a Member State regarding its implementation. If a directive is not (correctly) implemented, liability cannot exist solely based on that directive.[33] Ergo, rendering the sufficiency of the legal framework in light of the possibility to establish criminal liability.

The legality principle also encompasses the element of *lex certa*,[34] which constitutes the second factor to be considered. This principle serves as a guideline for legislatures, emphasising the need for individuals to be able to foresee what type of behaviour is considered illegal. As the Court of Justice of the European Union stated, 'the individual can know from the wording of the relevant provision, and if need be, with the assistance of the courts' interpretation of it, what acts and omissions make him criminally liable'.[35] Additionally, the law's text must provide adequate clarity to guide the judiciary in determining its scope of application.[36]

The third element of the legality principle relevant to this dissertation is *lex stricta*, which imposes specific limitations on the aforementioned interpretation by courts. While the law should be clear enough to guide the court, the judiciary is bound by the text of the law when interpreting its provisions.[37] Consequently, this principle prohibits analogical interpretation – where the law is applied to a similar situation not explicitly covered by the wording of the text – as well as (overly) extensive interpretation.[38] However, 'the gradual clarification of the rules of criminal liability through judicial interpretation from case to case, provided that the resultant development is consistent with the essence of the offence and could reasonably be foreseen',[39] is allowed.

Given the objective of this evaluative framework, the assessment does not determine if the existing legal frameworks are compatible with the aforementioned elements of the

---

31 *Kamerstukken II* 2003/04, 29702, 3, p. 85; Altena 2016, p. 95; Peristeridou 2015, p. 182. (Article 7 ECHR entails a broader concept of law. See: Altena 2016, p. 101).

32 Altena 2016, p. 103.

33 CJEU judgement of 26 September 1996, *criminal proceedings against Luciano Arcaro*, Case C-168/95; CJEU judgement of 7 January 2004, *criminal proceedings against X*, Case C-60/02; CJEU judgement of 3 May 2005, *criminal proceedings against Berlusconi and others*, Case C-387/02; CJEU judgement of 7 October 2010, *criminal proceedings against Martha Nussbaumer*, Case C-224/09.

34 The *lex certa* principle also requires that individuals can comprehend the law linguistically (i.e., it must be written in the official language) and that the law should be accessible (official publication). These aspects of the *lex certa* principle are not considered within the evaluative normative framework.

35 CJEU judgement of 3 June 2008, *The Queen on the application of: International Association of Independent Tanker Owners (Intertanko), International Association of Dry Cargo Ship Owners (intercargo), Greek Shiping Co-operation Committee, Lloyd's Register, International Salvage Union v. Secretary of State for Transport,* Case C-308/06, par. 71; CJEU judgement of 3 May 2007, *Advocaten voor de Wereld VZW v. Leden van de Ministerraad*, Case C-303/05, par. 50. See also ECtHR judgement of 25 March 1993, Series A/260, *Kokkinakis v. Greece*, par. 52; ECtHR judgement of 15 November 1996, *Cantoni v. France*, par. 29; ECtHR judgement of 21 October 2013, *Del Río Prada v. Spain*, par. 79.

36 Peristeridou 2015, p. 90.

37 Peristeridou 2015, p. 90-91.

38 Peristeridou 2015, p. 93-94.

39 ECtHR judgement of 22 November 1995, *SW v. The United Kingdom*, par. 36; See also CJEU judgement of 8 September 2016, *Merck KGaA v. European Commission*, Case T-470/13, par. 509-510.

legality principle. Instead, the focus is on evaluating whether establishing criminal liability on the same legal basis for new types of behaviour, namely cryptocrimes, would result in incompatibility with these elements of the legality principle. For European Union directives, which are not designed to directly establish criminal liability, the evaluation examines if the cryptocrime is typically covered by the minimum rules prescribed by the directive's framework.

For each identified cryptocrime, the assessment explicitly considers if there is a written law and, if applicable, whether it has been (correctly) implemented into Dutch national law in line with the *lex scripta* element. If this requirement is met, the evaluation proceeds by systematically identifying and analysing the legal components of the relevant legal framework.[40] Subsequently, what type of behaviour falls within the scope of the law in question is assessed based on a systematic review of the legislative process and applicable case law. Once this legal framework is established, it is evaluated whether its application to a specific type of cryptocrime would violate the *lex stricta* element and thus contravene the legality principle. Concerns regarding the foreseeability of applying the law to cryptocrimes are also considered under the *lex certa* element.

If issues arise concerning the establishment of criminal liability for the identified cryptocrime – irrespective of which element(s) 'prohibits' the application – the cryptocrime is deemed insufficiently regulated. In such cases, an evaluation using the desiderative normative framework follows to review whether additional regulation or amendments to the existing legal framework are necessary.[41]

4.2.1.2. Effective application

If the current legal framework has been found sufficient to establish criminal liability, the next step is to assess whether the application constitutes an effective practice. While legislation may not be designed with new or emerging technologies in mind, such technologies might fall within its scope by coincidence. Applying existing frameworks to novel situations may, however, prove impractical or result in unintended side effects. To address this, the second part of the evaluative normative framework reviews the application of a legal regime towards crypto-assets. This evaluation considers, among other factors, the unique characteristics of crypto-assets, such as anonymity, a decentralised set-up, the usage of cryptography and the irreversibility of transactions. Although some of these characteristics are present in 'established' instruments – such as anonymity in cash transactions and cryptography in Pretty Good Privacy – it is important to recognise that the combination of these characteristics is unprecedented and most legislation is not specifically designed for crypto-assets.[42] The effectiveness of a legal framework is assessed using the following criteria:

1. (Expected) goals,
2. Results,
3. Unintended side effects.

---

40 For further details on the methods of interpretation used in this dissertation, see § 4.2.1.3.

41 See § 4.2.2 for the desiderative normative framework.

42 See § 4.4 and 5, Chapter 2, for a detailed discussion of the unique characteristics.

These criteria are emphasised in the Dutch legislative process and also play a role in European regulation.[43] Certain criteria that may be relevant for new legislation, such as societal costs and the availability of alternatives for regulation, are not considered in this dissertation. Since cryptocrimes are, in general, a new manner of committing already existing crimes, omissions in legislation would undermine the legal frameworks already established for the non-crypto variant of these behaviours. In other words, the legislature has already decided that the non-crypto variant warrants regulation. Evaluating alternatives for regulation specifically for cryptocrimes would undermine this prior decision. Furthermore, societal costs are expected to have a minor influence on whether cryptocrimes are included in a legal framework as displacement from regulated to unregulated behaviour would diminish the effectiveness of the existing legal framework.

Below, I elaborate on the meaning of the relevant factors: (expected) goals, results and unintended side effects.

1) (Expected) goals

Legislation is always designed with one or more specific interests in mind. These objectives lie at the core of any legal regime and shape the entire legislative process.[44] In this discussion, it is relevant whether the (expected) goals of the legal framework align with the objectives of application to the cryptocrime.

The criminalisation of money laundering, for example, aims to protect the integrity of the financial and economic sectors.[45] Combatting money laundering involving crypto-assets presumably shares this aim, but is it reasonable to assume that application of the existing legal regime by definition leads to realisation of the same goal? In other words, distinct objects or technologies may necessitate different approaches to ensure the same objectives are met. If application of the current legal regime serves a conflicting goal or undermines its original aim(s), the framework will, in light of the paramount position the aim(s) have, be considered inefficient as a basis for establishing criminal liability regarding the cryptocrime.

2) Results

The outcome of using an existing legal regime to address a specific cryptocrime are evaluated. This assessment considers parliamentary discussions and academic literature on the envisioned result of the legislation in question. If the outcome for cryptocrimes deviates significantly from the originally intended results, the efficiency of the application is called into question.

Returning to the money laundering example: to prevent money laundering, Dutch and European legislation designates certain 'gatekeepers', such as banks, to implement prescribed measures.[46] Consider the scenario where Bitcoin also falls within the scope of these provisions. Unlike banks, Bitcoin operates on a decentralised, peer-to-peer

---

43 Recommendations for regulations (*Aanwijzingen voor de regelgeving*) *Stcrt*. 2017, 69426; Council conclusions on model provisions, guiding the Council's criminal law deliberations, 30 November 2009; European Parliament resolution of 22 May 2012 on an EU approach to criminal law, par. 3.

44 Recommendations for regulations (Aanwijzingen voor de regelgeving) *Stcrt*. 2017, 69426, chapter 1.

45 Recital 1-2 Directive 2015/849; *Kamerstukken II* 1999/00, 27159, 3, p. 5-6.

46 See Article 2 Directive 2015/849 (consolidated version); Article 1a Dutch Anti-Money Laundering and Anti-Terrorist Financing Act.

network where, for example, transactions are verified by 'individuals'. Applying the same rule set to this context would produce markedly different outcomes. The collective individuals in the network would bear responsibility for measures such as customer due diligence. Although the aim of prevention would still be addressed, it is highly doubtful that this practice aligns with the intent of the European Parliament and Council. The due diligence measures were deliberately assigned to banks, not to their customers. In such cases, the outcome would be considered to vary significantly from the intended original result.

3) Unintended side effects

Most (criminal) legislation and regulations have side effects which must be carefully examined during the legislative process.[47] Application of a certain legal regime to new technologies or objects may produce unintended side effects that were not anticipated during the legislative process. For each cryptocrime, an assessment is conducted to evaluate whether applying the existing regime results in such side effects. This evaluation takes a broad perspective, considering impacts on the system, users, technological foundations and the unique characteristics of crypto-assets.[48]

General guidelines for assessing secondary effects are unavailable as parliament typically evaluates each regulatory proposal on a case-by-case basis – albeit often implicitly. In the absence of objective criteria, the side effects of applying existing regimes to cryptocrimes are analysed in the context of discussions in academic literature and legislative history regarding the acceptability of such secondary effects.

This represents the most subjective element of the effectivity test. Therefore, appraisals regarding the significance of unintended side effects should be considered alongside the other elements before concluding that a legal regime is ineffective for addressing a specific cryptocrime.

It must be noted that a strict separation between the criteria is somewhat artificial. If applying a legal framework to a cryptocrime results in (the protection of) objectives that differ from those originally intended by the legislature, it is likely to also lead to unintended side effects and different results in application. However, distinguishing between the criteria – although slightly artificially – contributes to a more detailed and precise assessment.

4.2.1.3. Methods of interpretation

For the evaluative normative framework, it is essential to establish the substantive meaning of the selected provisions. To achieve this, various forms of interpretation are employed in this dissertation, which are elaborated on below.

---

47 Recommendations for regulations (Aanwijzingen voor de regelgeving) *Stcrt*. 2017, 69426, rec. 2.9.; Council conclusions on model provisions, guiding the Council's criminal law deliberations, 30 November 2009, p. 2; European Parliament resolution of 22 May 2012 on an EU approach to criminal law, par. 8.

48 During the parliamentary process, the side effects are assessed. When a framework enters into force, its general side effects are presumed to have been evaluated and considered acceptable. Consequently, this review focusses on the secondary effects that are unique to crypto-assets.

i) Textual interpretation
This method of interpretation involves using the everyday meaning of a term or its definition in dictionaries to clarify its substance within the legal context.[49] The text of a legal framework often serves as the starting point for interpreting a specific element.[50] This method is recognised in various legal systems, including those of the European Union and the Netherlands.[51]

ii) Systematic interpretation
This interpretation method, often referred to as the 'contextual interpretation' method, considers a provision within the broader context of the legal system and legal framework to which it belongs.[52] It acknowledges that a specific legal provision does not exist in isolation or can be explained in a vacuum but is always part of a larger system (and context) that must be taken into account.[53] In many legal systems, including those of the European Union and the Netherlands, this interpretation method is used.[54]

iii) Teleological interpretation
Teleological interpretation, also known as 'purposive interpretation', focusses on the intended effect of the law.[55] It emphasises the purpose of a legal framework, as derived from the choices made by the legislature.[56] This method is commonly applied in both the European Union and the Netherlands.[57]

iv) Historical interpretation
The historical interpretation method focusses on the circumstances that existed when the legal framework was enacted.[58] The meaning of a specific element is understood in its historical context to establish its definition.[59] While this method is widely used, it is less prevalent in the European Union.[60]

Each of the interpretation methods have been criticised for various reasons. For instance, with regard to the textual interpretation method, critiques have pointed out that the definition of a word in everyday use is not always clear and depends on the context in which it is used. The systematic interpretation method could place an excessive burden on the judiciary, the teleological method may be subjective as the intent of the legislature is not always clear, and the historical interpretation may fail to provide insight into the legislature's intent at the time.[61]

---

49 Ammann 2019, p. 197.
50 Hullu, de 2024, p. 117.
51 Klip 2021, p. 149; Hullu, de 2024, p. 117-118.
52 Ammann 2019, p. 202.
53 Hullu, de 2024, p. 119; Ammann 2019, p. 202.
54 Klip 2021, p. 149-150; Hullu, de 2024, p. 119.
55 Ammann 2019, p. 208.
56 Hullu, de 2024, p. 119-120.
57 Kristen 2004, p. 15-16; Hullu, de 2024, p. 119-120.
58 Ammann 2019, p. 213.
59 Cf. Kristen 2004, p. 18-20.
60 Klip 2021, p. 156-159; Hullu, de 2024, p. 118.
61 Ammann 2019, p. 198-214.

Interpretation methods are often used in conjunction with one or more other methods. For example, the European Court of Justice frequently combines the textual method with the systematic and teleological interpretation, particularly when language versions conflict.[62] Combining these techniques of interpretation may mitigate some of the critiques associated with specific interpretation methods. Where possible in this dissertation, I combine multiple methods of interpretation to substantiate the meaning of elements.

4.2.1.4. Schematic overview

An overview of the evaluative normative framework is included in Figure I.

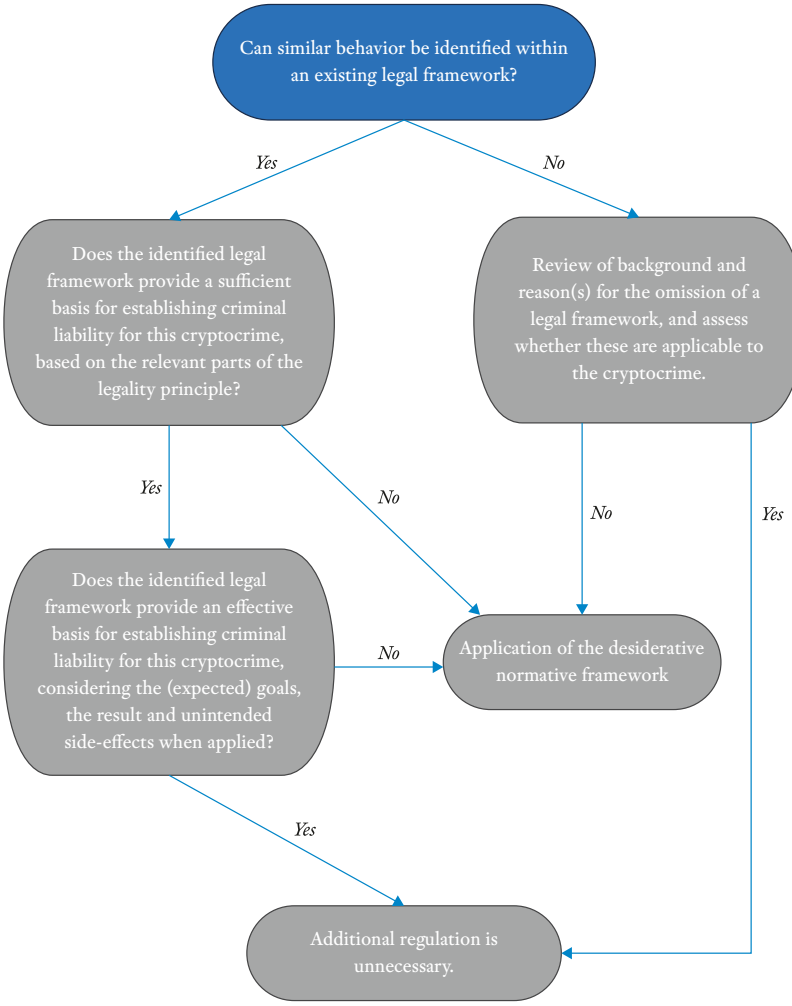

Figure I: Overview of the evaluative normative framework.

[62] See Klip (2021, p. 149-152) and the case law cited there. See also Ammann 2019, p. 220 for a recommendation on the combined use of interpretative methods.

4.2.2. *Desiderative normative framework*

If the current legal regime is considered insufficient or inefficient based on the evaluative normative framework, the desiderative framework will assess whether a modified approach or legal framework could resolve the identified complication(s). The next section details the concept of crypto and non-crypto equivalence, which is central to the desiderative normative framework. § 4.2.2.2 discusses the practical application of the normative framework.

4.2.2.1. Crypto and non-crypto equivalence: Background

The desiderative framework is based on the assumption of crypto and non-crypto equivalence. This concept arises from an analogical interpretation of online and offline equivalence. In essence, this idea refers to a shared foundation for rules in both the online and offline realms. Given this common ground, the law should not differ between these domains in terms of effects and/or wording. It advocates for neutrality between equal activities, regardless of the realm in which they manifest.[63] This principle is recognised in Dutch and European regulatory processes and is the basis of numerous laws concerning technological developments.[64]

By adopting the principle of crypto and non-crypto equivalence as a guiding axiom to strengthen the regulatory framework, this analysis maintains a strong connection to existing legislation. Current laws reflect the legislature's perspective on crime. During the legislative process, proposed laws must undergo thorough evaluation, although this is sometimes implicit. Using existing legal frameworks as a template for 'equal' behaviour preserves a connection to the current state of criminalisation. If cryptocrimes threaten the protected interests underlying these legal frameworks, it can be assumed to be beneficial – from a criminal policy perspective – to regulate cryptocrimes as well. Therefore, the concept of 'necessity' for regulating crypto-asset related crimes and abuse, as used in this dissertation, is closely linked to the past considerations and intentions of the legislature; this understanding of necessity benefits the consistency of the law.

Criteria for criminalisation[65] are useful for assessing which behaviour should be criminalised. They may, however, have limited value when it comes to additional regulation of behaviour already considered illicit by the legislature. When legislation is already in place, why introduce unnecessary abstraction in regulating what is clearly defined? The concept of crypto and non-crypto equivalence offers additional benefits over criteria for criminalisation. Notions on criminalisation have a political dimension and may change over time, which could render certain criteria for criminalisation obsolete. On the one hand, existing legislation often reflects the prevailing political priorities and dynamics. On the other hand, the results of a review based on equivalence should be reassessed if the basis (i.e., the non-crypto regulation) for comparison changes. While criteria for criminalisation must evolve to reflect shifting principles and contemporary perspectives within criminal law, the concept of equivalence focusses on the changed legislation itself.

---

63 Schellekens 2006, p. 58; Reed 2010, p. 250-251.

64 E.g. Schellekens 2006, p. 54; Reed 2010, p. 248-249, 252-253. A more recent example can be found in the Regulation on Markets in Crypto-Assets (see Recital 9).

65 E.g. Hulsman 1972; Bemmelen, van 1973; Feinberg 1990; Roos, de 1987; Haveman 1998.

Furthermore, criteria for criminalisation are often bound to specific levels. For example, the formulation of legislation at the Dutch level generally requires different criteria than regulation at the European level. In contrast, crypto and non-crypto equivalence starts with the original legislation in each individual jurisdiction. The concept of equivalence is dynamic, evolving as societal norms, technologies and circumstances change. On the other hand, criteria for criminalisation are often static; once created, they typically remain unaltered. In light of these considerations, this manuscript favours the use of crypto and non-crypto equivalence over criteria for criminalisation.

Nevertheless, the question remains: Why is equivalence desirable? Imposing diverging legal regimes on crypto and non-crypto situations could create the impression among the public that there is a distinction in what behaviour is considered acceptable. As Reed points out, in the context of online and offline equivalence, this requires individuals to make a 'mental switch' in how they view what is unwanted or inappropriate behaviour – an impractical expectation.[66] In this regard, the principle of crypto and non-crypto equivalence emphasises the need to justify deviations or comparable regimes for these realms, based on the view of what actions should be considered equivalent.

In practice, the principle of equivalence can refer to various uses.[67] In this dissertation, it is used in two ways. First, it acts as a starting point to assess non-crypto rules and the comparability of non-crypto and crypto behaviour.[68] In this context, the principle serves as a guideline to assess whether situations can be considered equal by comparing the underlying interests of regulation and the harm the behaviour caused.

The second aspect of the principle concerns the drafting technique of legal frameworks. If there is equivalence between non-crypto and crypto behaviour, it must be regulated equally.[69] However, the principle, particularly in relation to the concept of online and offline equivalence, is not always applied in a distinct and consistent manner in definitions of 'equal'. Sometimes 'equal' refers to formal equivalence, which pertains to the applicability of certain legislation to equal situations; in other words, the text of the rule does not distinguish between crypto and non-crypto behaviour. In other instances, it refers to the effect of a rule. Although its wording may differ for the crypto world and the non-crypto world, legislation must have the same consequences for both. This is known as functional equivalence.[70]

The concept of formal equivalence has not been without criticism. It is often associated with technology neutrality,[71] a related principle to online and offline equivalence. Using the same wording to address both the crypto and non-crypto worlds may result in laws

---

66 Reed 2010, p. 253. See also: Recommendations for regulations (*Aanwijzingen voor de regelgeving*) *Stcrt*. 2017, 69426, rec. 2.10.

67 Schellekens 2006, p. 56.

68 Cf. Schellekens 2006, p. 56 & 66.

69 Schellekens 2006, p. 56.

70 Reed 2010, p. 251.

71 Closely related to the principle of online and offline equivalence is the principle of technology neutrality. At the heart of this guiding axiom is a non-discriminatory approach to technology. However, interpretations of this principle vary. Neutrality towards technology may refer to formal equivalence, functional equivalence or both. Unlike the principle of offline and online equivalence, technology neutrality is often emphasised as a means of 'futureproofing the law' for emerging technologies. Given that this dissertation is limited to crypto-assets, a certain degree of technological

that produce legal uncertainty as they lack clarity and (implicitly) impose different regimes on the two realms.[72] The main challenge associated with functional equivalence is how to achieve comparable outcomes given the inherent differences between the two dimensions.[73]

4.2.2.2. Crypto and non-crypto equivalence: Contextual application

The desiderative framework builds on the selection of relevant existing European and Dutch legal frameworks, as identified in sub-questions 1 and 2. This initial collection focusses solely on the factual similarities between crypto-asset and non-crypto-asset behaviour. Under this framework, it is assessed whether the identified insufficiency or ineffectiveness necessitates the modification of the legal framework or the introduction of additional legislation. Two pathways emerge: i) The non-cryptocrime is unregulated and therefore no legal framework exists; ii) the non-cryptocrime is regulated, but the existing legal framework is insufficient or inefficient in addressing the cryptocrime in question. Both pathways are detailed below.

i) A legal framework is absent

How should the assessment proceed if comparable behaviour has not been regulated? This depends on the reason for the omission: is the observed behaviour unique to crypto-assets, or was the comparable non-crypto behaviour deliberately left unregulated? A preliminary assessment suggests that the likelihood of identifying behaviour unique to crypto-assets is currently minimal. As explained in § 1 of this chapter, contemporary cryptocrimes can be divided into two categories: i) abusive behaviour related to the issuance and trading of crypto-assets, and ii) the facilitation of crime. From a legal perspective, the acts primarily involve the introduction of a new object and new (related) markets. While the technology is groundbreaking, the conduct enabled by crypto-assets is not.[74]

If the conduct is deliberately left unregulated, the starting point, given the presumption of equal treatment, should be that there is no necessity to regulate the cryptocrime. An evaluation of the reasons for permitting the behaviour follows to assess how these reasons apply in connection to the cryptocrime. The focus is on the underlying interests of (de)regulation and the unique characteristics of crypto-assets and their market. This assessment may lead to the conclusion that regulation of the cryptocrime may be necessary due to inherent differences to the system.

An example may clarify this point. Certain actions are not regulated at the European Union level due to the principle of subsidiarity.[75] These behaviours typically involve physical objects and therefore remain within the borders of individual Member States. Now, imagine that these objects are replaced with crypto-assets, which can be easily transferred across borders. In this case, Member States may have differing regulatory

---

differentiation is inherent. Consequently, technology neutrality is not the primary focus and plays only a secondary role. Recommended readings: Reed 2007; Greenberg 2016; Koops 2006.

72 Reed 2010, p. 250; Koops 2006, p. 90; Greenberg 2016, p. 1557.

73 Reed 2010, p. 252.

74 If unique cryptocrimes emerge in the future, they can be reviewed against the criteria for criminalisation. E.g. Hulsman 1972; Bemmelen, van 1973; Feinberg 1990; Roos, de 1987; Haveman 1998.

75 See Article 5, paragraph 3, Treaty on European Union (TEU).

regimes, potentially leading to 'forum shopping' by criminals. Would the principle of subsidiarity still be an obstacle to creating legislation in such circumstances?

ii) A legal framework is identified

A legal framework is initially chosen under the evaluative normative framework because the behaviour it pertains to shares factual similarities with the identified cryptocrime. Following the concept of crypto and non-crypto equivalence, the next step involves assessing whether there is true legal equivalence between the situations; this is because only equal behaviour should be regulated 'equally'.

First, this is ascertained by identifying the underlying interests that the existing regulation aims to protect or serve and comparing these to the goals of criminalising the crypto-variant. If the interests differ, the situations cannot be considered equal. Cryptocrimes should therefore only be recommended for regulation if the protected interests align substantially with those of the selected existing laws and regulations.[76]

Next, the type and volume of the harm caused by crypto and non-crypto behaviour is compared. By assessing the harm caused by cryptocrimes relative to their non-crypto equivalent, insights can be gained regarding the harm the legislature seeks to prevent through regulation. It is also possible to evaluate whether the harm caused by the cryptocrime calls for equal treatment. It is likely that the type of harm will be of a financial nature in both variants, but a direct comparison is made to confirm this initial presumption. The volume of harm, such as the financial value or the number of victims affected in a single case, may differ between the realms. By comparing the magnitude of harm observed in individual cases, it can be determined whether the cryptocrime causes harm of at least the same extent. If the volume of harm in crypto-cases is lower than in the selected non-crypto counterpart, it must be evaluated whether the protected interests of the specific regulation are still served by regulating the cryptocrime, or whether it should remain unregulated.

Most criteria for the criminalisation or regulation of unwanted behaviour include factors related to the type of instrument or field of law best suited for regulation.[77] The lack of such criteria in the desiderative normative framework stems from the presumption of crypto and non-crypto equivalence. Deviating in the field of law or the type of instrument may create the undesirable perception that different norms apply when acting in a cyber environment.[78] However, there may be valid arguments for selecting a different type of instrument for the regulation of cryptocrimes, as seen in legislation addressing various technological developments. While the field of law and the type of instrument connected to the regulated non-crypto behaviour guide the regulation of crypto-assets related crimes and abuse in this dissertation, the specific instrument should be evaluated more comprehensively during parliamentary discussions or in further research on this topic.

---

76 Inspired by Dutch jurisprudence on the interpretation of 'same fact' in relation to the *ne bis in idem* principle: HR 1 February 2011, *NJ* 2011/394 m.nt. Buruma; HR 18 June 2019, *NJ* 2019/463 m.nt. Reijntjes.

77 E.g. Hulsman 1972, p. 3-21; Bemmelen, van 1973, p.7-14; Feinberg 1990, p. 1-24; Roos, de 1987, 58-60; Haveman 1998, p. 43-94.

78 Reed 2010, p. 253; Schellekens 2006, p. 53.

If the behaviour is considered to require regulation, the study proceeds with recommendations for how European and Dutch legislation could be amended to effectively counter cryptocrimes. Using the principle of crypto and non-crypto equivalence as a substantive guideline ensures that the core principles underlying existing legislation applicable to comparable non-crypto-assets, such as e-cash and fiat currencies, are taken into account. In line with the principle of crypto and non-crypto equivalence and the primary aim of strengthening the legal framework for cryptocrimes – namely, preventing crime displacement and deterring opportunistic offenders – the starting point of the desiderative normative framework is regulation of the cryptocrime in the same manner (formal equivalence) and with the same effects (functional equivalence). In this dissertation, functional equivalence is not limited to legal side effects but also encompasses broader side effects, such as the impact on the technique and system of crypto-assets. If this leads to reformulating existing legislation, it must be evaluated whether the amendments would alter the practical application and effects of the non-crypto variant.[79]

Using the same wording for online and offline behaviour may lead to dissimilar effects, as previously mentioned. The unique characteristics of crypto-assets may, for example, necessitate deviations in regulation. Some characteristics of crypto-assets, such as anonymity (which can also be found in cash money) or the use of cryptography (as seen in software like Pretty Good Privacy), are not new. Instead, it is the combination of those characteristics, along with a decentralised set-up and the degree of irreversibility of transactions inherent in crypto-asset systems, that pose novel dynamics.[80] Given the criticism of formal equivalence, I believe that the interests concerned with avoiding unjust or unbalanced outcomes should outweigh the perceived benefits of using identical wording to include cryptocrimes and other behaviours. If formal and functional equivalence cannot be achieved, functional equivalence should, consequently, take precedence. In such cases, the existing regulation serves as a template, and the least textually divergent option that fulfils functional equivalence is recommended.[81]

4.2.2.3. Schematic overview

An overview of the desiderative normative framework is included in Figure II.

79 Reed 2010, p. 251.
80 See § 5-6, Chapter 2.
81 Schellekens 2006, p. 73.

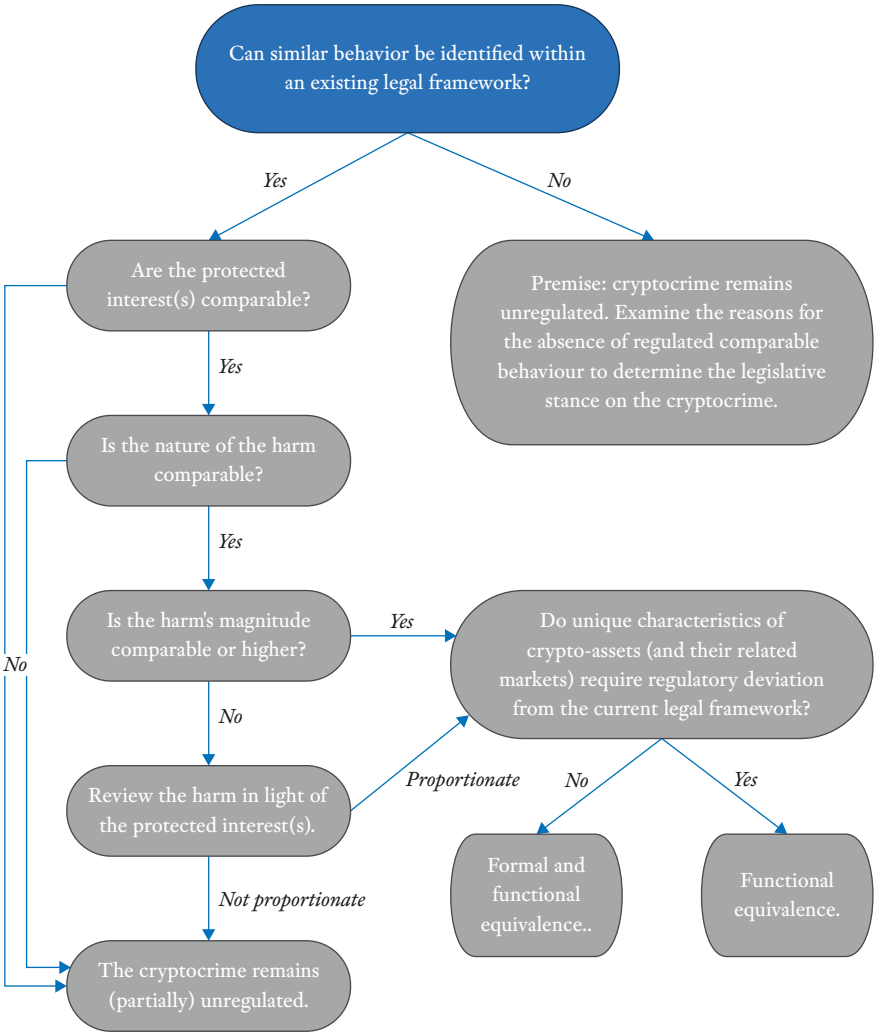

Figure II: Overview of the desiderative normative framework

5. Scope and limitations

As indicated in the central research question, the scope of this dissertation is confined to the European and Dutch levels. While the societal challenge of cryptocrimes is inherently international, this study focusses exclusively on the Dutch and European contexts. A comprehensive global analysis of the legal status of all types of cryptocrimes is not feasible due to constraints on time, linguistic proficiency, and in-depth knowledge of the various legal systems worldwide. Therefore, a thorough and fundamental analysis of cryptocrimes within these jurisdictions is favoured over a global perspective. By

integrating both the European Union and Dutch levels, this research acknowledges the multi-layered nature of legislation.

The concept of crypto and non-crypto equivalence is not without its limitations. Since it depends heavily on existing legislation, any amendments to the original non-crypto regulation will inevitably affect the evaluation of how cryptocrime variants should be regulated. While the findings derived from the desiderative framework are up to date as of the time of publication, they may require reassessment in the future to account for legislative changes. Additionally, the concept of equivalence also poses limitations concerning the selection of the most appropriate regulatory instrument for addressing specific cryptocrimes, as discussed in § 4.2.2.2.

The concrete recommendations formed in this dissertation are inherently tied to existing legislation as they are based on the principle of crypto and non-crypto equivalence. Consequently, these recommendations cannot be generalised beyond the jurisdiction for which they were formulated, namely either the European Union or the Netherlands. However, this dissertation retains value outside these jurisdictions. The desiderative normative framework, with its open and adaptable character, can be applied in other legal systems. That said, it may prove less suitable for common law legal systems due to its strong reliance on legislative processes and the considerations of legislatures.[82] The scope for the descriptive part of the dissertation – addressed by sub-question 1 – is broader. It is not confined to the Netherlands or the European Union,[83] allowing the identified types of cryptocrimes to be generalised to a significant degree.

As stated, this dissertation focusses on 'criminal offences' and, as such, addresses only one segment of the challenges that crypto-assets pose to the area of criminal justice. This study is specifically concerned with the grounds for criminal liability and is therefore limited to substantive criminal law and punitive administrative law. Other areas, such as procedural criminal law and penalties, are not dealt with in this study. Given the vast number of potential cryptocrimes, it is not feasible to discuss all aspects of the criminal justice system. As the investigation of cryptocrimes and the subsequent punishment for a cryptocrime are only possible if there is an existing basis for criminal liability, it is imperative to clarify which cryptocrimes are covered by substantive criminal law. Future research on procedural criminal law and penalties concerning cryptocrimes can build on the findings presented in this dissertation.

In addition, this monograph only examines a specific area of law. For example, issues of a civil nature or more abstract concerns such as developing a universal definition of crypto-assets fall outside the scope of this dissertation. The range of these topics is too broad to be adequately covered within a single book. Attempting to combine them would result in a dissertation that could not do justice to any of the issues this technology raises. By focussing on 'criminal offences', this dissertation explores a subset of the problem, ensuring a coherent and thorough analysis of the topic.

---

82 Given the trend toward codification of criminal law even in common law jurisdictions, the desiderative normative framework may prove useful. See Peristeridou 2019, p. 94-96.

83 Due to my linguistical limitations, only sources written in Dutch, English or German are considered.

6. Currency of this book

Developments occurring after [1 March 2025] have not been taken into account.