Smart Contracts and Corrective Justice: What Contract Law Can and Cannot Do

Cormac Kilkenny, B.C.L., LL.M.

Thesis Submitted for the Award of Doctor of Philosophy

School of Law and Government, Dublin City University

Supervisors:

Dr. Rónán Condon

Dr. John Quinn

August 2026

Declaration

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of Doctor of Philosophy is entirely my own work, and that I have exercised reasonable care to ensure that the work is original and have conformed to the regulations on the use and declaration of Generative AI, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

I hereby certify that no Generative Artificial Intelligence (Gen AI) tools have been used in the creation of the thesis.

Signed: Cormac Kilkenny

Cormac Kilkenny

ID No.: 16379153

Date: 25 August 2026

Acknowledgments

First, I would like to thank my supervisors, Dr. Rónán Condon and Dr. John Quinn. From the very beginning, they recognised the potential in my research and have provided invaluable encouragement and insight throughout the process. I also wish to thank Mr Justice Mateja Durovic for making me feel truly welcome during my visit at King's College London. Many thanks also to the Reed family for the warm hospitality during my time in London; you truly enriched my experience in London and I am very grateful.

I am grateful for my scholarships, as they have made it possible for me to pursue the research for this thesis. I am particularly thankful for the research funding generously provided by Research Ireland under Grant GOIPG/2023/4692. My thanks also to the School of Law and Government at DCU.

I also wish to acknowledge the advice and support I received from the staff at DCU. A special thanks to Head of School Dr. Tanya Ní Mhuirthile, Prof. Yvonne Daly, Dr. Goran Dominioni, Dr. Christy Petit, Dr. James Gallen, Dr. Emma McEvoy, and Dr. Róisín Costello.

Thanks also to friends both inside and outside DCU. Special thanks to Padraic, Paul K., Paul M., Aoife, Lauri, and Matt, who have offered much encouragement during the last four years. Thanks also to Simon, Mengting, Marcel, Seán, Lia, and Liam.

I’m grateful for Valerie, George, Eric, and Albert. Thanks for making me a part of the family, giving me a home away from home, and always offering words of encouragement.

Sincere thanks to my family, extended and immediate. I especially want to acknowledge my parents, Deirdre and Fintan, who have been such a vital support throughout this process. Pursuing a Ph.D. can be challenging, and they’ve always been there to listen during both the

highs and lows. From the very start of my academic path, their support has meant the world to me. Whether I was celebrating a success or venting about a challenge I was facing, they always had the kettle boiled. I want to express my gratitude to my brother Andrew for being the supportive big brother he is, and for always looking out for me.

And finally, I want to share my heartfelt appreciation for my partner, Harriet, who has been by my side throughout the entirety of this journey. Seeing her excel as a Ph.D. researcher has been a constant source of inspiration for me. I am so thankful to have such an amazing, kind, and supportive partner to share this path with.

Table of contents

Acknowledgments....3

Abbreviations....11

Abstract....12

1 Introduction....13

1.1 Introduction....13

1.2 Research question....20

1.3 Thesis outline and structure....21

2 A Corrective Justice Theory of Smart Contracts....24

2.1 Introduction....24

2.2 Corrective justice....26

2.2.1 Alternative theoretical accounts of contract law: non-instrumentalism and instrumentalism....26

2.2.2 'New Private Law' theories....29

2.2.3 What is corrective justice?....31

2.2.4 Why corrective justice?....35

2.3 Coherence of contract law....39

2.4 Correlativity....46

2.4.1 Gains and losses....46

2.4.2 Bilateral structure of right and duty....48

2.5 The regulatory-instrumentalist discussion versus the ongoing need for private law 50

2.6 Conclusion 55

3 From Paper to Digital Agreements: The Formation of Smart Contracts 57

3.1 Introduction 57

3.2 Contract rulebook 61

3.2.1 Offer 61

3.2.2 Invitation to treat 63

3.2.3 Unilateral and bilateral contract distinction 64

3.3 Acceptance 65

3.4 Consideration 66

3.5 Intention to create legal relations 67

3.6 Legal validity of smart contracts 68

3.6.1 Parameters affecting the mapping of smart contracts to corrective justice 69

3.7 Formation of smart contracts 72

3.7.1 Identifying an offer and acceptance in bilateral smart contracts 73

3.7.2 DASC offers and acceptances 75

3.7.3 Advertisements on crypto asset marketplaces 79

3.7.4 The irrevocable agreement 80

3.7.5 DAO Offers and acceptances 83

3.7.6 The Legal Classification of DAOs 89

3.7.7 The Nature of DAO Contracts: Multilateral Smart Contracts 92

3.7.8 Offer and Acceptance of the Coded Contracts of DAOs 93

3.8 Consideration in smart contracts 98

3.8.1 Bilateral smart contract consideration 100

3.8.2 DASC consideration 101

3.8.3 DAO consideration 103

3.9 Intention to create legal relations in smart contracts 104

3.9.1 Intention to create legal relations in bilateral smart contracts 104

3.9.2 Intention to create legal relations in DASCs 106

3.9.3 Intention to create legal relations in DAOs 108

3.10 Conclusion 111

4 From Paper to Protocol: Interpreting Smart Contracts Under Traditional Contract Law 112

4.1 Introduction 112

4.2 Principles of interpretation 113

4.3 Interpreting Parallel Agreements: The Smart Contract and Natural Language Document 116

4.4 Interpreting Code: Smart Contracts in Isolation 119

4.4.1 Interpreting DAO smart contracts 123

4.5 Conclusion 125

5 Voiding the Digital Deal?: Assessing the Smart Contract for Vitiation 127

5.1 Introduction 127

5.2 Mistake 129

5.2.1 Common mistake 129
5.2.2 Unilateral mistake 132
5.3 Frustration 134
5.4 Misrepresentation 137
5.5 The vitiation of smart contracts 142
5.6 Smart contracting mistakes 143
5.6.1 Unravelling Mistake in BSCs 143
5.6.2 Mistake in DASCs 146
5.6.3 DAO mistake 152
5.7 Misrepresentations in smart contracts 156
5.7.1 Bilateral smart contract misrepresentation 156
5.7.2 DASC misrepresentation 159
5.7.3 DAO misrepresentation 164
5.8 Frustration of smart contracts 166
5.8.1 Frustration and Force Majeure in Bilateral Smart Contracts 166
5.8.2 DASC frustration 171
5.8.3 DAO frustration 175
5.9 Conclusion 178
6 The Limitations of Contract Remedies: Assessing Where Traditional Remedies Succeed and Fail in Smart Contracts 179
6.1 Introduction 179
6.2 Breach of contract and damages 183

6.2.1 Breach in bilateral smart contracts 185
6.2.2 The DASC and the inadequateness of damages 187
6.2.3 Breach of DAO smart contracts 190
6.3 Specific performance 192
6.3.1 Specific performance in bilateral smart contracts 194
6.3.2 Specific performance and the DASC 197
6.3.3 Specific performance in DAOs 200
6.4 Rescission 201
6.4.1 Rescission of bilateral smart contracts 204
6.4.2 Rescission in DASCs 208
6.4.3 Rescission of DAO smart contracts 212
6.5 Rectification 214
6.5.1 Bilateral smart contract rectification 215
6.5.2 Rectification of DASC transactions 219
6.5.3 DAO smart contract rectification 221
6.6 Injunctions 223
6.6.1 A serious issue about smart contracts? 224
6.6.2 Bilateral smart contract injunctions 225
6.6.3 Injunctions in the DASC context 226
6.6.4 Injunctions against DAOs 229
6.7 Terminating the smart contract 230

6.7.1 Bilateral smart contract termination....230
6.7.2 Repudiation and termination of a DASC....232
6.7.3 Termination of a DAO smart contract....235
6.8 Conclusion....236
7 Unjust Enrichment: A Response for the Non-Contractual DASCs and DAOs....238
7.1 Introduction....238
7.2 Principles of unjust enrichment....240
7.3 Unjust enrichment and DASCs....243
7.4 Unjust enrichment and DAO smart contracts....249
7.5 Conclusion....252
8 Conclusion....254
Bibliography....264

Abbreviations

B2B - Business-to-business

P2P - Peer-to-peer

DAO - Decentralised Autonomous Organisation

DASC - Decentralised Anonymous Smart Contract

MiCAR - Markets in Crypto Assets Regulation

NFT - Non-fungible token

Abstract

Smart Contracts and Corrective Justice: What Contract Law Can and Cannot Do

Cormac Kilkenny

Smart contracts are an autonomous mode of transacting online which may challenge the law of contract. This thesis examines how smart contracts map on to the concepts of corrective justice through the law of contract. It draws on Ernest Weinrib's theory of private law which centres on the juridical relationship, emphasising the roles of the plaintiff and defendant in private law disputes. A taxonomy of smart contracts is proposed to evaluate the limitations of corrective justice in rectifying wrongs within such transactions. The 'bilateral' smart contract, expressed partly in natural language, aligns with corrective justice as the correlative rights and duties of the parties are easily discerned. Here, the smart contract functions as a mechanism used to bring about the parties' self-determined purposes. In contrast, The 'decentralised anonymous' smart contract (DASC), which relies primarily on computer code to negotiate and perform its terms, obscures the role of the parties and diminishes their capacity as self-determining agents, making legal enforceability of the DASC uncertain. The third form of smart contract concerned in this thesis derives from the decentralised autonomous organisation (DAO). Constituted by a web of multilateral smart contracts used to manage the assets and governance of the organisation, the DAO renders it difficult to identify the correlativity and bipolarity necessary to ground a claim in contract law. Ultimately, this thesis reveals the existence of contract law's limitations as a means to obtain corrective justice when humans rely on code to manage their interactions. It concludes that the law of unjust enrichment may be better suited to respond to DASCs as it may apply when a contract is absent, but a normative loss is nevertheless sustained by the plaintiff. Potential regulatory-instrumentalist interventions are also considered where the regulative capacity of the law of contract is exhausted. In articulating its position, the thesis adopts a common law perspective, and draws upon the laws of Ireland, England and Wales, Singapore, New Zealand, Australia, and the United States. By adopting a common law approach, this thesis articulates a broad theory of smart contracting, the findings of which may be mapped onto alternative jurisdictions where similar private law concepts have been established.

1 Introduction

1.1 Introduction

A new market has grown out of the creation of blockchain technology, wherein greater focus has been placed on the exchange and value of digital assets. Cryptocurrencies and non-fungible tokens (NFTs) have received significant attention globally, and the market for these new classes of digital assets have endured several bubbles and crashes. Although much attention has been placed on the speculative assets available to users in the current version of the Web, the real value derives from the fact that users are no longer 'passive consumers' and have better opportunities to participate and contribute within the digital community.[1] Ultimately, the blockchain narrative can be summed up as an attempt to encode trust within software, therefore displacing the need for lawyers and the courts, or brokers and banks.[2] The conduct of the community is predominantly governed by computer code which dictates which actions users can and cannot perform. To get to this point, the community required new methods of transacting with one another. Consequently, the Ethereum blockchain adopted the use of smart contracts as a method to facilitate transactions. Nick Szabo, a cryptographer and legal scholar, conceptualised the smart contract in 1994.[3] His vision was fully realised when the Ethereum blockchain introduced the use of smart contracts as the medium to facilitate transactions. Smart contracts became useful in this regard because they can manipulate digital assets, most often in the form of cryptocurrencies and NFTs.[4]

[1] Joseph Lee and Jyh-An Lee, 'Roadmap to Legal Implications of Web3: An Introduction' in Lee J and Lee J-A, *Web3 Governance: Law and Policy* (Routledge 2025).
[2] Eliza Mik, 'Smart Contracts: Tales of Trust and Certainty' (2022) 2022 Technology and Regulation 100, 102–103.
[3] Nick Szabo, 'Smart Contracts' (*Universiteit van Amsterdam*, 1994) <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> accessed 3 July 2023.
[4] Jason Grant Allen, 'Wrapped and Stacked Smart Contracts' in Jason Grant Allen and Peter Hunn (eds), *Smart Legal Contracts: Computable Law in Theory and Practice* (Oxford University Press 2022) 32.

Ultimately, the thesis concludes that smart contract agreements expressed entirely in computer code may not be contracts at all because the parties may not comprehend the coded terms until they have been executed and fully performed. Lacking an understanding of the code's output means that the smart contract may not be a manifestation of the parties' self-determining agency because their capacity for self-determination has been outsourced to the software's code. However, this does not mean that parties who suffer losses because of such smart contracts must always bear their losses. The final substantive chapter concludes that those parties may instead turn to the law of unjust enrichment where contract law fails to provide parties with the means to rectify the injustices of their code-produced transactions. In articulating its approach, the chapter provides an alternative way of deciding the case of Quoine Pte Ltd v B2C2 Ltd, in which the Singaporean Court of Appeal denied the appellant a remedy because the transaction was brought about by the algorithms of the two involved parties.5 This finding that unjust enrichment should rectify the injustice caused in Quoine also applies to other smart contract arrangements. Two other archetypes of code-only smart contracts are examined to test this finding, including the sale of the CryptoPunk #2386 NFT and the 'DAO hack'. Ultimately, the finds that the law of unjust enrichment, rather than contract law, may be used in response to such smart contracts where a natural language agreement is absent.

Corrective justice remains at the core of the law of unjust enrichment because transactions must 'manifest or reflect the autonomy of the person who is making the payment'.[6] Unjust enrichment may be relied upon by the plaintiff where it may be denied that a smart contract is a contract at all, but where there has been a normatively defective transfer of value.[7] This way, the transactional imbalance may be rectified notwithstanding the lack of a contract between the

[5] *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA (I) 02.
[6] Andrew Botterell, 'Property, Corrective Justice, and the Nature of the Cause of Action in Unjust Enrichment' (2007) 20 Canadian Journal of Law & Jurisprudence 275, 286.
[7] *Revenue and Customs v Investment Trust Companies* [2017] UKSC 29 [42].

parties, all while adhering to the correlativity of the parties' positions.[8] As such, the thesis concludes that the law of unjust enrichment is the avenue through which the plaintiff may coherently recover his normative losses resulting from smart contract transactions.

There are several purported benefits to using smart contracts instead of traditional contracts. They reduce transaction costs by removing intermediaries such as lawyers and brokers. The code within the smart contract enforces the parties' agreement, therefore negating the need for traditional methods of contract enforcement by the courts. They are secure because, once executed, the transaction is memorialised on the blockchain and the record is tamper-proof. They are transparent because their code is publicly visible and can therefore be reviewed by prospective parties. However, their legal character has been the subject of ongoing academic debate, the question at the core of which asks whether they are legal contracts, or merely forms of software which manipulate digital assets.[9]

Some of the approaches which scholars have used to-date include the analysis of smart contracts through the contract 'as consent', and 'as promises' theories.[10] The former theory centres on the promisor's manifested intention to create legal relations. The outward manifestation of intention may be absent because parties may execute smart contracts without intending or knowing that they have.[11] Regarding the latter theory, smart contracts may not constitute promises at all because they render performance inevitable.[12] The act of promising is obsolete because the contract is performed by computer code rather than by human hands. Corrective justice offers a better alternative to the consent or promissory theories of contract

[8] Ernest J Weinrib, *Corrective Justice* (Oxford University Press 2012) 189.
[9] For an argument that smart contracts are not enforceable contracts, see Eliza Mik, 'The Sense and Nonsense of Smart Contracts' (Social Science Research Network, 2 September 2024) 8 <https://papers.ssrn.com/abstract=5189279> accessed 20 May 2025.
[10] For these well-known contract theories, see Randy E Barnett, 'Consent Theory of Contract' (1986) 86 Columbia Law Review 269, and see Charles Fried, *Contract as Promise: A Theory of Contractual Obligation* (2nd edn, Oxford University Press 2015).
[11] Farshad Ghodoosi, 'Contracting in the Age of Smart Contracts' (2021) 96 Washington Law Review 51, 65–66.
[12] Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 67 Duke Law Journal 313, 356.

by focusing objectively on the parties' mutual manifestations rather than on one-sided ideas of promises or consent. This thesis argues that the corrective justice theory of contract is a suitable lens through which to assess smart contract transactions. Not only does corrective justice explain why a contract comes into existence, it also seeks that the interaction between the parties is fair and equal. It aims to identify the entitlements of the parties involved (i.e 'what is rightfully theirs') based on whether the defendant has gained more than he should have, and if the plaintiff has lost more than was acceptable under the contract.[13]

The fairness and equality provided by corrective justice is a result of its aspiration towards coherence. To be coherent, the parties' relationship must be structured correlatively, and accordingly, a justification ought not to favour one party over the other.[14] In contract law understood from a corrective justice perspective, parties are empowered to establish legal relations with whoever they so wish, provided that the relationship is consistent with their equal freedom.[15] An unjust transaction according to corrective justice is one where the defendant infringes the equality between the parties, thereby obtaining a gain, and through the same interaction inflicts a loss on the plaintiff.[16] In sum, corrective justice provides contract law both with its structure *and* its normative content by offering a remedy to the plaintiff when the defendant infringes his right to contractual performance.

This thesis problematises smart contracts from a corrective justice purview. To test this argument, I adopt a taxonomy of three smart contract types. The first type of smart contract, the *bilateral smart contract*, involves a plain language agreement which precedes the software

[13] Ernest J Weinrib, 'Corrective Justice in a Nutshell' (2002) 52 The University of Toronto Law Journal 349, 344–355.
[14] Ernest J Weinrib, 'Legal Formalism' in Dennis Patterson (ed), *A Companion to Philosophy of Law and Legal Theory* (John Wiley & Sons, Ltd 2010) 332.
[15] Andrew Botterell, 'Corrective Justice and Contract Law' in Mindy Chen-Wishart and Prince Saprai (eds), *Research Handbook on the Philosophy of Contract Law* (Elgar Publishing 2025) 107.
[16] Weinrib, 'Corrective Justice in a Nutshell' (n 13) 354–355.

smart contract that expresses the terms of the parties' agreement.[17] This type of smart contracting arrangement provides the same level of clarity as traditional contracts, and the purpose of the code is mainly to perform all, or part of, the agreement. The *in personam* right of enforcement is acquired in the same way as in a conventional contract through the process of offer, acceptance, and consideration. This way, the parties may be integrated in a 'unified but bipolar relationship' which is affirmed by the passing of consideration from the offeree.[18]

In contrast, the *decentralised anonymous smart contract (DASC)* may not so easily confer a right of performance on the plaintiff. In this type of smart contract, the code of the software purportedly creates and enforces the right of performance.[19] For various reasons, this affects the compatibility of the DASC with corrective justice. One of this is that corrective justice requires that there is a correlative duty to each right, however there purportedly is no duty for the defendant to fulfil as the contract handles performance itself.[20] Additionally, it may be unclear as to what are the correlative rights and duties of the parties because these are expressed entirely in computer code. Normatively unjust transactions may not be unwound however if the offeror argues that the code of the DASC constitutes the terms of the agreement.[21] This calls into dispute whether a DASC is a contract at all, and if so, how a remedy may be obtained by a party who has suffered a normative loss under it.

The final mode of smart contracting of which our taxonomy is comprised are *decentralised autonomous organisation* (DAO) smart contracts, where the purpose of the software is not to alter the rights and duties of two parties, but to create the infrastructure for a whole virtual organisation. These are virtual organisations hosted on the blockchain which 'exist

[17] This type of smart contract was considered by Brownsword in Roger Brownsword, 'Regulatory Fitness: Fintech, Funny Money, and Smart Contracts' (2019) 20 European Business Organization Law Review 5, 21.
[18] Ernest J Weinrib, *The Idea of Private Law* (Oxford University Press 2012) 137–138.
[19] Nataliia Filatova, 'Smart Contracts from the Contract Law Perspective: Outlining New Regulative Strategies' (2020) 28 International Journal of Law and Information Technology 217, 234.
[20] Werbach and Cornell (n 12) 340.
[21] Ghodoosi (n 7) 80.

autonomously' and require human interaction only for activities that cannot be achieved using automation.[22] To exist autonomously, they rely on a nexus of smart contracts, the code of which automates the DAO's processes, including the payment of software developers and other participants responsible for the DAO's maintenance. Given the network of participants required to run a DAO, it is likely that secondary and tertiary contracts will be required to coordinate those actors. The concepts of corrective justice become strained when mapped against DAO smart contracts because of the number of participants involved, therefore potentially affecting the requirement of correlativity. Moreover, the smart contracts used in DAOs are often used to manage its inner workings and do not create legal relations. However, many DAOs are established for commercial purposes and will therefore involve some transactions internally and externally to the organisation.[23]

The literature often focuses on the regulatory-instrumentalist approach to smart contracts. Broadly speaking, this methodology prioritises the law's efficiency in achieving specified regulatory goals as opposed to its coherence.[24] The conversation often centres on the ex ante management of risk, for instance, by regulating the 'architecture' of the blockchain.[25] However, this approach, which relies on legislative intervention by the state, overlooks the smart contract as a means of private ordering. The smart contract aims to establish a horizontal bilateral nexus between two parties by effecting a transaction of digital assets. As such, the smart contract falls under the domain of private law, which is juridical rather than political in nature.[26] In testing smart contracts using contract law in its 'purest' form, this thesis is not concerned with the

[22] Vitalik Buterin, 'DAOs, DACs, DAs and More: An Incomplete Terminology Guide' (*Ethereum Foundation*, 6 May 2014) 5 <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide> accessed 17 July 2024.
[23] For example, see David M Grant, Eric M Kirby and Steven R Hawkins, 'Decentralized Autonomous Organizations: To Statutorily Organize or Not?' (2024) 24 Wyoming Law Review 59, 73.
[24] Roger Brownsword, 'Regulatory Fitness: Fintech, Funny Money, and Smart Contracts' (2019) 20 European Business Organization Law Review 5, 12.
[25] For example, see Primavera de Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 181.
[26] Ernest J Weinrib, *The Idea of Private Law* (Oxford University Press 2012) 8.

legislative or regulatory interventions that may be made by the state in regard to smart contracts. Instead, it takes seriously the 'fundamental concepts' of contract law which concern the direct connection between the plaintiff and defendant, as opposed to the independently justifiable objectives that may be advanced by the state.[27]

However, this thesis is not alone in treating smart contracts through the lens of contract law.[28] Where it differs however, is in its analytical approach. By adopting a corrective justice approach, it is not limited to doctrinal application, and may assess the ability of smart contracts to render a bilateral connection between the parties based on the essential components of private law. The analysis therefore goes beyond merely testing the fit between smart contracts and contract law's doctrines as it also examines whether smart contracts align with private law's character, kind, and unity. As these aspects exhibit the intelligibility of private law, it is necessary to refer to them to illuminate contract law in its purest form.

Although crypto asset markets have been the target of public regulation, contract law retains an important role in ensuring corrective justice in smart contract transactions. By the end of December 2024, the European Union's Markets in Crypto Assets Regulation (MiCAR) came into effect with a view to regulate the growing crypto asset markets.[29] Its method of regulation targets gatekeepers in the form of crypto asset service providers (CASPs). Some of the measures included in the Regulation mandate that CASPs publish a white paper detailing their services, the risks involved in trading their assets, and the rights and obligations including investor entitlements and token holder privileges. However, MiCAR does not regulate crypto

[27] ibid.

[28] For example, see Mateja Durovic and André Janssen, 'Formation of Smart Contracts under Contract Law' in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019); Nataliia Filatova, 'Smart Contracts from the Contract Law Perspective: Outlining New Regulative Strategies' (2020) 28 International Journal of Law and Information Technology 217; Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 67 Duke Law Journal 313.

[29] Regulation (EU) 2023 of the European Parliament and of the Council 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.

asset services that are 'fully decentralised'.[30] While the Regulation captures large actors within the crypto market (e.g. FTX, Binance, Coinbase), it overlooks other areas where transactions may occur such as peer-to-peer marketplaces, and interparty transactions. These transactions remain within the domain of contract law.

1.2 Research question

The purpose of this thesis is to determine how the smart contract maps onto contract law's concepts and rules. In answering this question, contract law and the smart contract are viewed through the lens of corrective justice judging the smart contract in three different contexts. The first is the bilateral smart contract which entails a natural language agreement and a coded smart contract to perform the parties' relatively straightforward agreement. The second is the DASC which expresses and performs the parties' agreement in computer code. The third is the DAO, which involves a multiplicity of smart contracts which are used to create a virtual organisation governed by autonomous code. It examines how the parties' rights and duties may arise under these smart contract categories, and subsequently, how contractual injustices may occur which warrant correction through contract liability. It discusses the extent to which this rectification is possible, with a view to ultimately determine in what smart contracting contexts corrective justice may be obtained.

The thesis ultimately finds that bilateral smart contracts pose few challenges for corrective justice through the law of contract. The reason is that the courts need only refer to the natural language agreement to ascertain the correlative rights and duties of the parties, from which the remedy may be determined. However, DASCs are problematised because of the absence of this natural language agreement. When the parties delegate the power of formation and

[30] ibid, Recital (22).

performance of their agreement to autonomous computer code, it becomes less evident that the contract represents a manifestation of equal freedom, as engaged by two self-determining agents. When code makes decisions and performs on behalf of the parties, their capacity for self-determination is diminished. As such, they may not know the terms of their interaction until after it has been fully performed, or the rights and duties they acquire. This may make it difficult for the courts to determine whether the smart contract can, or should be, void or voidable. It may also be difficult to grant a remedy that will rectify the defendant's normative losses because it may not be possible to identify a norm or right that has been infringed. Finally, DAO smart contracts may be particularly challenging because they are often multipartite contracts involving the interests of several third-parties. If the courts grant a remedy for one of the DAO's smart contracts, that remedy may affect the other interconnected smart contracts that constitute the DAO. Nevertheless, DAO smart contracts are also often expressed entirely in the form of computer code and the rights and duties of the parties and the ability to interpret them may be difficult. They therefore stretch the limitations of corrective justice and contract law in its existing form, and may require legislative intervention to clarify the standing of DAO participants.

1.3 Thesis outline and structure

Chapter two sets out the corrective justice framework that is applied to smart contract transactions throughout the thesis. Corrective justice provides both the structural and normative content of contract law, wherein the equality of the parties and the fairness of their transaction is central.

Chapter three identifies characteristics unique to smart contracts that may broadly affect how well they map on to corrective justice. The fact that they are immutable, may sometimes be

expressed entirely in code, and made by anonymous parties, are potential factors which affect how they fit with corrective justice. The chapter then outlines how smart contracts may be established under the doctrines of formation. Bilateral smart contracts are similar to conventional contracts because they are expressed in natural language before they are executed using a coded smart contract. Therefore, the parties may form a juridical relationship by clearly setting out the terms to which they agree to be bound. In contrast, DASCs may evade the creation of such a relationship because they are expressed in the form of code only. As such, the parties' purposes may be opaque so as to render offer and acceptance difficult.

Chapter four argues that the parties' mutual will may be objectively ascertained in a bilateral smart contract by looking to the natural language document of the parties agreement and the surrounding context of the transaction, while the interpretation of the DASC yields difficulties that may prevent the courts from identifying the parties' objective purposes.

Chapter five outlines the vitiation of smart contract agreements. It argues that the vitiation of the parties' agreement may be more easily identified in a bilateral smart contract owing to the existence of a natural language agreement where their rights and correlative duties may be found. Where these rights are automated and expressed in code, it may be more difficult to identify the vitiation of the parties' agreement.

Chapter six finds that the remedies of contract and equity may in principle apply neatly to bilateral smart contracts, but struggle on a practical basis to restore the parties to a pre-contractual position in line with the requirements of corrective justice. The limits of remedies are more pronounced where the transaction is immutable and in the form of code (such as in DASCs and DAOs).

Chapter seven discusses how the law of unjust enrichment provides a better course of action for parties who suffer losses through DASCs and DAO smart contracts. Although the thesis is

fundamentally concerned with the law of contract, it is through unjust enrichment that the plaintiff may recover their losses where a contract does not exist.

Chapter eight concludes the thesis by providing a brief discussion about the alternative potential responses to smart contracts to negate the harm caused by the correlative normative gains and losses of smart contracting parties.

2 A Corrective Justice Theory of Smart Contracts

2.1 Introduction

Smart contracts – computer programmes that automatically execute transactions according to predetermined conditions set out in their source code – present unique challenges to traditional contract law principles.[31] The courts may have some difficulty in applying contract law principles and remedies to smart contracts because of the typical characteristics of these software-based agreements. For instance, the immutability, pseudonymity, and lack of any natural language agreement involved in some smart contract transactions may render them difficult to interpret and enforce.

This chapter sets out the theoretical framework that will be applied throughout this thesis. It draws specifically on a corrective justice theory of contract law that excludes functionalist considerations like the economic objectives of the law, and focuses instead on contract law from a formalist perspective. Under the formalist view, private law is understood as an autonomous discipline which is objective and apolitical.[32] Specifically, it is Weinrib's theory of private law which views contract law as inherently formalist, coherent, and states that it aims to achieve corrective justice. In particular, this thesis examines whether contract law can fit with a corrective justice theory of contract. Based on its formalism, the framework focuses heavily on the body of contract law doctrine and principles. More specifically under this paradigm, private law transactions are comprised of bilateral relationships between parties where one party's right correlates with the other's duty. It is this correlativity which serves as private law's 'supreme regulative principle'.[33] Thus, the normative position of one party is only

[31] Allen (n 4) 32–33.
[32] Morton J Horwitz, 'The Rise of Legal Formalism' (1975) 19 The American Journal of Legal History 251, 256.
[33] Ernest J Weinrib, *Reciprocal Freedom: Private Law and Public Right* (Oxford University Press 2022) 8.

intelligible relative to the position of the other party. As such, this framework takes into consideration the correlative gains and losses attributable to the parties' interactions, and the reciprocal rights and duties of those parties toward one another.

The framework discounts considerations beyond those which affect the immediate parties, and therefore distances itself from the concerns which occupy functionalist accounts of contract law. For instance, wealth maximisation, deterrence, and community welfare (among other things) are at the centre of various functionalist theories.[34] Broadly speaking, the functionalist is concerned with the broader social interest of judicial outcomes, rather than the legal interests of the two parties who are directly concerned as part of an interaction. Although applying a functionalist paradigm to smart contracts may yield interesting results, the focus centres on the private law relationship, and the remedies that flow from same. This is because civil liability under the corrective justice model is 'an entirely interactional phenomenon' wherein a specific defendant is always liable to a particular plaintiff.[35] Thus, contract law should be examined according to its own structure, of which this chapter provides an account.[36]

Functionalist theories are not the only accounts that disregard the nature of the private law relationship in this manner. There are also formalist accounts of contract law that do not treat to the structure of the parties' relationship as unified. For example, Fried's *Contract as Promise* has the makings of a formalist theory because it does not concern itself with broad societal interests and instead homes in on the parties' individual rights.[37] However, it disregards the nature of the private law relationship by centring on the duty of the promisor to act as he had promised. Due to its lack of focus on the right obtained under the contract by the promisee,

[34] Weinrib, *Idea* (n 14) 4.
[35] Ernest J Weinrib, 'The Corrective Justice of Liability for Unjust Enrichment' in Elise Bant, Kit Barker and Simone Degeling (eds), *Research Handbook on Unjust Enrichment and Restitution* (Edward Elgar Publishing 2020) 168.
[36] Peter Cane, 'Corrective Justice and Correlativity in Private Law' (1996) 16 Oxford Journal of Legal Studies 471, 472.
[37] Fried (n 6).

Fried's theory does not address the correlative nature of the juridical relationship. In a similar way, Barnett's formalist theory does not take into account the bipolar relationship of contracting parties because it is concerned with the one-sided consideration of consent given by the transferor for the purpose of the exchange.

This chapter first argues why corrective justice is a worthy paradigm through which smart contracts will be examined. Private law generally, and contract law particularly, takes the form of corrective justice, and competing instrumentalist accounts fail to recognise it. Secondly, it provides an overview of corrective justice, which emphasises the correlativity of the private law relationship. It then explains this correlativity in the form of the bipolar gains and losses, and rights and duties of the parties. It then discusses the coherence of contract law. It then addresses the 'regulatory-instrumentalist' discussion and states why private law is still a necessary mode of regulating smart contract transactions.

2.2 Corrective justice

2.2.1 Alternative theoretical accounts of contract law: non-instrumentalism and instrumentalism

Various theories have been published in the last century which strive to explain the nature of contract law. These theories range from those which treat contract law as non-instrumentalist to those that argue that it is instrumentalist in its outlook. A non-instrumentalist theory of contract law is centred on the will of the parties and is not concerned with welfare or other external considerations that do not impact the parties' immediate interaction.[38] Instrumentalists on the other hand argue that contract law is concerned with efficiency or distributive justice.

[38] Peter Benson, 'The Idea of a Public Basis of Justification for Contract' (1995) 33 Osgoode Hall Law Journal 273, 278.

Non-instrumentalist theories of contract law generally find that law and politics are two disparate fields. In contrast, instrumentalists assume that law and politics cannot be separated.[39] I will briefly outline some of these accounts before discussing the theory which informs the theoretical framework for this thesis.

A recognized theory of contract law, as articulated by Charles Fried, posited that the primary purpose of contract law is to reinforce moral obligations through the establishment of corresponding legal obligations.[40] He argued that contract law is all about individual rights, and that it is less concerned with the collective interests of society as a whole. Therefore, it is closer to a formalist account of contract law as it is non-instrumental. However, in referring to the morality of promises as the driving factor of contract law, Fried fails to recognise private law's structure. Under his theory, the structure is one-sided as only the promisor undertakes a duty to perform because she is morally obligated to do so. This however does not reflect the bilaterality of the private law relationship which provides the promisee with a correlative right.[41] The requirement that the promisor keeps his promise provides the parties with their correlative right and duty. Contract law doctrines of offer, acceptance, consideration and the remedy of expectation damages show how the plaintiff's right is embraced along with the defendant's duty.[42] As Weinrib argues, any theorist who argues that contract law is premised predominantly on morality ought to 'illuminate' this structure otherwise their theory may provide an 'inadequate' account of contract.

An alternative theoretical account of contract law is provided by Randy Barnett, which argues that contract is based on the manifestation of the parties' intention to alienate their rights.[43] However, similarly to Fried, Barnett's theory does not illuminate private law's structure

[39] Felipe Jiménez, 'Two Questions for Private Law Theory' (2021) 12 Jurisprudence 391, 406.
[40] Fried (n 6) 14–17.
[41] Weinrib, *Idea* (n 14) 51.
[42] ibid.
[43] Barnett (n 6) 304.

because it is founded on the one-sided consideration of consent. Under this view, consent moves only from the party who has undertaken to transfer his rights to the transferee.[44] However, the plaintiff and defendant are correlatively linked by their conduct as rational agents with self-determined purposes. The parties' interactions in contract are reciprocal rather than one-sided.[45]

Then there are the reliance theories of contract such as those advanced by Fuller and Perdue, and Patrick Atiyah. The underlying idea is that contracting carries with it a risk that the person who relies on the contract may be made worse off due to their reliance.[46] Fuller and Perdue argue that by entering a contract, the person who relies on the contract obtains a 'reliance interest'. The reliance interest protects plaintiffs who alter their position because of the promise made by the defendant, and who subsequently incurs a loss.[47] The reliance interest places such parties in a position as though they did not rely on the promise. Murphy argues that this version of reliance theory is overly extensive, giving an example of a party who was 'induced' to buy a plane ticket to Australia because the other party stated publicly that he was also bound for Australia.[48] As such, the reliance interest includes considerations that are beyond the parties' transaction. For instance, under the reliance theory, harm to the plaintiff may include the opportunity cost of entering into the contract.[49] Drawing on Murphy's example, the induced party may have travelled elsewhere to somewhere she preferred over Australia. However, there was no connection of the parties' wills so as to provide the induced party with a contractual right.[50] In contract law, the parties' respective yet mutual wills are linked through the doctrines

[44] Andrew S Gold, 'A Property Theory of Contract' (2009) 103 Northwestern University Law Review 1, 26.
[45] Weinrib, *Corrective Justice* (n 8) 152.
[46] Stephen A Smith, *Contract Theory* (Oxford University Press 2004) 78.
[47] LL Fuller and William R Perdue, 'The Reliance Interest in Contract Damages: 1' (1936) 46 Yale Law Journal 52, 54.
[48] Liam Murphy, 'The Practice of Promise and Contract' in Gregory Klass, George Letsas and Prince Saprai (eds), *Philosophical Foundations of Contract Law* (OUP Oxford 2014) 161.
[49] Fuller and Perdue (n 41) 54.
[50] For discussion of the 'expectation interest' of which this thesis applies, see Section 2.2.3.

of formation. However, the doctrines of offer and acceptance are not concerned with the plaintiff's reliance, but whether there has been an agreement between the parties through which they have manifested their self-determining agency.

2.2.2 'New Private Law' theories

There are alternative accounts of private law which view it as the manifestation of the parties' self-determination situated within the 'New Private Law' movement. New Private Law theory is characterised by its treatment of private law on its own terms while willing to consider both internal and external points of view.[51] Although there are many academics who comprise the NPL collective, this thesis draws upon the work of Dagan and Dorfman who provide one of the most developed forms of NPL in relation to the law of contract. In particular, they argue that private law is concerned with the horizontal relationship between two parties united in a particular transaction.[52] This stance so far reflects the formalist position. However, the formalist and the NPL positions diverge in how they view the private law relationship. While the formalist sees private law as committed to the purposive agency of the parties and formal equality, Dagan and Dorfman view it as devoted to 'individual self-determination and substantive equality'.[53]

In this articulation of private law, substantive equality aims to take the parties 'for the persons they actually are'.[54] To attain substantive equality, the parties' terms of interaction accounts for their circumstances as well as their constitutive choices regarding their 'ground projects'. Only by doing so will private law respect the parties' capacity to act as self-determining agents. The parties are not treated as independent beings bipolarly situated in their

[51] Andrew S Gold and others (eds), 'Introduction' *The Oxford Handbook of the New Private Law* (Oxford University Press 2020) xv.
[52] Hanoch Dagan and Avihay Dorfman, 'Justice in Contracts' (2022) 67 The American Journal of Jurisprudence 1, 7.
[53] ibid 19.
[54] ibid 8.

interaction, but are viewed as participants in a cooperative endeavour which may render them more vulnerable to one another.[55]

Although this framing of private law resembles the corrective justice theory, it may be distinguished for various reasons. In terms of their similarity, both theories appeal to the parties' purposiveness as the underlying rationale of contracting.[56] Parties enter agreements with their own pursuits in mind and in doing so, form a unified interaction. Both theories are concerned with the horizontal relationship of the parties, and therefore recognise the distinction between public law and private law. However, the theories differ because Dagan and Dorfman prioritise the substantive equality of the relationship (along with the parties' self-determination) over formal equality.[57] This framework diverges from formalist theories of corrective justice, which maintain that private law is an apolitical, autonomous realm, which should remain insulated from substantive commitments beyond the relationship's internal structure.[58]

Private law's apolitical state derives from the requirement of its own coherence.[59] A judgment may be coherent if it does not allude to the desirability of a specific legal relationship.[60] However, drawing upon the substantive merits of the relationship upsets the formal equality between the parties. Accordingly, corrective justice disclaims considerations of the parties' social ranks or moral character because the inclusion of such factors may render the parties unequal.[61] To introduce these considerations into the equation would involve looking beyond the correlative aspects of the unified transaction, thereby rendering the relationship

[55] ibid 9–10.
[56] Ernest J Weinrib, 'The Normative Structuralism of Corrective Justice' in Hanoch Dagan and Benjamin C Zipursky (eds), *Research Handbook on Private Law Theory* (Edward Elgar Publishing 2020) 498.
[57] Hanoch Dagan and Avihay Dorfman, 'Just Relationships' (2016) 116 Columbia Law Review 1395, 1399.
[58] Weinrib, *Idea* (n 14) 25.
[59] For further discussion of the coherence requirement, see Section 2.3.
[60] Weinrib, *Idea* (n 14) 45.
[61] ibid 81.

incoherent. The factors that may be introduced in a private law dispute are those that apply equally to both parties.[62]

Dagan and Dorfman argue that private law should account for external factors that would affect one party's standing within the relationship. These factors include, for example, the party's disability, sex, or race.[63] Substantive equality is achieved by drawing upon the circumstances specific to the interacting parties. But in doing so, private law advances public law-styled objectives such as human flourishment, equality, and liberty, rather than focusing on the specific factors that link the parties. The introduction of an external standpoint to the private law relationship diminishes its intelligibility.[64] For this reason, the thesis adopts the Weinribian framework of corrective justice because it is pure in its focus on the juridical relationship of the contracting parties through its exclusion of such extrinsic factors.

2.2.3 What is corrective justice?

Corrective justice rectifies an injustice which the defendant has caused to the plaintiff.[65] It is concerned with the inequality of the parties' positions created by the transaction, and excludes concerns of resource allocation in society more broadly. This indicates the bipolarity of private law which can be traced through the private law process. For instance, the bilateral relationship between plaintiff and defendant begins at the point of their interaction, where one party has suffered an injustice and the other has caused that injustice. Following the point at which harm occurred, the plaintiff who suffered sues the particular defendant who caused him to suffer.[66]

[62] Ernest J Weinrib, 'Defending the Juridical' (2025) Canadian Journal of Law and Jurisprudence 1, 2-3.
[63] Dagan and Dorfman, 'Just Relationships' (n 57) 1418.
[64] Weinrib, *Idea* (n 14) 49.
[65] Weinrib, 'Corrective Justice in a Nutshell' (n 13) 349.
[66] Weinrib, *Idea* (n 14) 63.

Corrective justice then informs the remedy that applies to the single transaction that links the plaintiff and defendant. Considering that the initial gains and losses experienced by the parties involved in the private law transaction are mutually related, the injustice is rectified by imposing a loss on the defendant and granting a corresponding gain to the plaintiff.[67] Private law therefore is a distinct mode of ordering through corrective justice where the plaintiff and defendant are both connected in a unified transaction. They are connected through their correlative positions as doer and sufferer of the same harm.[68] The actions of one party are not considered in isolation.

Until now, corrective justice has been discussed insofar as it provides the form of private law. Without developing this account of private law further, the theoretical framework would be incomplete.[69] Therefore, Weinrib states that Kantian right provides the normative content which complements corrective justice's structure. Under this view, right is the 'juridical manifestation of self-determining agency'.[70] Private law therefore ensures that individuals can act freely without violating the freedom of others. A rule is justified if it articulates the self-determining freedom of both parties involved.[71] The technological shift of smart contracts foreground the principle of self-determining agency whereby parties enter into smart contracts with the expectation that their autonomous choices (which are manifested in code) will be respected and executed as agreed. In this sense, smart contracts operationalise the Kantian right by guaranteeing the contracting parties' freedom to contract is realised without interference.

[67] ibid 65.
[68] ibid 73.
[69] Weinrib found a lacuna in Aristotle's account of corrective justice: 'Despite his achievement, however, Aristotle's exposition, like all great pioneer efforts, is seriously incomplete. Aristotle presents corrective justice as a transactional equality, but he does not tell us what the equality is an equality of.' Ernest J Weinrib, 'Corrective Justice' (1991) 77 Iowa Law Review 403, 404.
[70] Weinrib, *Idea* (n 14) 81.
[71] Weinrib, *Corrective Justice* (n 8) 155.

In contract law, the nature of the right is such that the promisee acquires a right against the promisor to perform the act for which the parties contracted.[72] If the promisor breaches the contract, corrective justice corrects the transactional imbalance through expectation damages. It is through expectation damages that the courts restore the status quo because they provide the plaintiff with the value of performance had the defendant not breached the contract.[73] It is in this way that the courts impose a loss on the defendant, and a gain on the plaintiff by shifting the value of the performance back to him.

Alternatively, the injustice can be undone using an order of specific performance against the buyer, requiring that he does exactly what it is he promised to do in undertaking the obligation.[74] This would simply mandate the buyer to purchase the impugned asset, while also acknowledging certain limitations on the applicability of specific performance in a particular contractual scenario.[75] Additionally, a plaintiff's right to performance is not extinguished because the defendant failed to perform the contract by the time stipulated in the contract. In such instances, the defendant's duty becomes one to perform the contract promptly, thus downplaying the significance of the original breach.[76] Therefore, if a smart contract fails to perform as the parties voluntarily agreed it should, the courts may provide an order of specific performance, requiring that the smart contract is reperformed.

The expectation measure of corrective justice has been challenged by Fuller and Perdue as a 'queer kind of compensation' because it entitles a plaintiff to something which he never in fact

---

[72] ibid 153.

[73] Contract law does not aim to punish defendants because the act of punishment requires the courts to fixate on the conduct of one party. However, as will be discussed, contract law is concerned with the bilateral nature of the transaction and must therefore account for the actions of both parties. See Pey-Woan Lee, 'Contract Damages, Corrective Justice and Punishment' (2007) 70 The Modern Law Review 887, 892.

[74] Weinrib, *Corrective Justice* (n 8) 154.

[75] These limitations are discussed in greater detail, and applied to smart contracts in Chapter 5. It is sufficient to say here that these limitations include where damages are adequate and where the enforcement of the contract would require ongoing supervision.

[76] Stephen A Smith, 'Remedies for Breach of Contract: One Principle or Two?' in Gregory Klass, George Letsas and Prince Saprai (eds), *Philosophical Foundations of Contract Law* (OUP Oxford 2014) 344.

had.[77] Their argument is based on a framing of expectation damages as a remedy which protects the plaintiff's future expectancy rather than compensating them for a loss already suffered. They argue that the resulting remedy is distributive in nature rather than corrective. From this perspective, expectation damages serve a social function by enabling commerce and encouraging economic activity.

However, Fuller and Perdue's account does not take into account the nature of the right. The plaintiff was always entitled to the performance promised by the defendant, and it is irrelevant that the plaintiff never held the subject matter of the contract.[78] The difference between these two accounts is the way in which they treat the parties' relationship. Fuller and Perdue prioritise the protection of reliance and commercial convenience and in doing so treat the parties as means to an end. Their focus overlooks the fact that rights ensure that one self-determining party's actions are consistent with the freedom of the other.[79] Contract law remains fundamentally concerned with securing the promised performance, or compensating the plaintiff in accordance with the value of performance. Therefore, corrective justice remains committed to the intelligibility of private law and how it is structured in the law's own terms.[80] We therefore examine how an infringement of one's rights may manifest in a smart contracting context instead of considering matters of commercial convenience. Rather, we identify (if possible) the right contained in the smart contract, and how computer code may result in a breach of that right.

[77] Fuller and Perdue (n 41) 53.
[78] Weinrib, *Corrective Justice* (n 8) 154.
[79] ibid 155.
[80] ibid 155–156.

2.2.4 Why corrective justice?

Corrective justice not only provides contract law with its structure, but it also provides it with its normative content. The private law relationship is correlatively structured in a way that enables the courts to find liability. The normativity of corrective justice theory flows from its structure because by treating the parties as directly correlated to one another, they are viewed as equals wherein the courts may only draw on considerations that relate to them both as doer and sufferer of the same injustice.[81] Through its commitment to the structure and equality of the parties' interaction, corrective justice illuminates the fairness of a given transaction without reference to 'intuitive judgments of fairness' or fairness of how resources are to be distributed to society more broadly.[82] Instead, by focusing on the bipolar positioning of the parties within their interaction, corrective justice identifies a fair outcome and renders liability accordingly. Liability takes the form of an *ex post* remedy that adjusts the parties' holdings to by providing the plaintiff with that to which he was entitled according to their mutual agreement.

However, the rigid automation of smart contracts purportedly negates the need for ex-post remediation by the courts by rendering breach impossible or costly.[83] Alternatively, when a smart contract does cause harm and result in a dispute, some may argue that the smart contract's output is legitimate and its beneficiary is entitled to keep the benefit gained under it because computer 'code is law'.[84] If this is true, and smart contracts do obviate the need for the courts, then they may be the antithesis of corrective justice. The reason is that the courts have an essential role in correcting any imbalances in the equality of the parties' transaction resulting

[81] Ernest J Weinrib, 'The Normative Structuralism of Corrective Justice' in Hanoch Dagan and Benjamin C Zipursky (eds), *Research Handbook on Private Law Theory* (Edward Elgar Publishing 2020) 487.
[82] ibid.
[83] JG Allen, 'Wrapped and Stacked: "Smart Contracts" and the Interaction of Natural and Formal Language' (2018) 14 European Review of Contract Law 307, 313.
[84] Under the 'code is law' approach, software and hardware together govern how users interact in cyberspace. See Lawrence Lessig, *Code 2.0: And Other Laws of Cyberspace* (Basic Books 2006) 5. For an example of how the 'code is law' argument was advanced in the blockchain context, see Karen Yeung, 'Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law' (2019) 82 Modern Law Review 207, 234.

from the defendant's conduct.[85] Given that smart contracts involve reciprocal commitments between the parties, one party may potentially default on his side of the bargain. Corrective justice provides smart contracting parties with recourse to the courts if their smart contract does not reflect the self-determined purposes of their interaction.[86]

The strength of the corrective justice approach is found in its focus on addressing the imbalance of equality within parties' transactions. It does so by providing a reason to assign rights and duties to parties in transactions. These correlative rights and duties indicate when parties have made a normative loss and normative gain that necessitates the courts' intervention.[87] If the defendant has obtained a normative gain at the expense of the plaintiff, corrective justice enables the courts to rectify the losses incurred by the plaintiff.[88] In so doing, the courts may restore the notional equality that existed prior to the parties' interaction by providing the plaintiff with that which he is owed.[89] By applying corrective justice theory to smart contracts, the objective of this thesis is to determine how the courts may still protect the purposive agency of smart contracting parties through contract law.

Private law, and therefore contract law, has a form which is distinct from other forms of legal ordering. Corrective justice is '*the* form of private law', while distributive justice characterises public law.[90] Corrective justice offers the best explanation of contract law because it is most in line with the essence of contract law. Therefore, it is used in this thesis as a method to filter out considerations external to the law and to focus strictly on components internal to contract law. By applying a corrective justice theory, this thesis explains whether certain smart contracts are

[85] Weinrib, *Idea* (n 14) 65.
[86] ibid 105.
[87] The difference between a factual gain/loss versus a normative gain/loss is discussed at Section 2.4.1. For now, it is sufficient to say that a normative gain by the defendant and a normative loss by the plaintiff attracts liability. Factual or material gain and loss do not.
[88] Weinrib, *Corrective Justice* (n 8) 16.
[89] Botterell (n 15) 108.
[90] Weinrib, *Idea* (n 14) 55. Emphasis added.

in fact contracts, or are things which exist beyond contract law's scope. However, this requires that we accept as a starting point that contract law is formalist rather than functionalist, and that its form is corrective justice.

The idea that contract law has a particular form can be traced back to the Aristotelian account of justice. Corrective justice applied to voluntary and involuntary transactions; the former being the domain of today's law of contract, and the latter constituting torts.[91] It rectifies injustices which arise between parties by depriving one party of an unjust gain and returning it to the harmed party. Contract law achieves this in a particular manner by identifying a juridical relationship governing the transaction. The contract law dispute takes the form of corrective justice through its correlative structure. The defendant does, and the plaintiff suffers, the same harm. Through the principal doctrines of contract law, parties can be bound together in this unified relationship.[92] In this sense, the doctrines of offer, acceptance, and consideration, seek to establish a bilateral relationship between the parties, whereby one party puts out an offer which her counterparty accepts. By undertaking this process, the parties' actions place them as opposites in the same transaction. The doctrine of consideration further establishes the bilateral nexus between the two parties because it requires correlative acts by both the promisor and the promisee.[93] It is insufficient that the promisor acts unilaterally, and as such a contract will not be created. Correlative conduct is necessary to result in a contract.

The elements discussed in the preceding paragraphs point to contract law's intelligibility.[94] Contract law has a form in which intelligibility is important because the law places demands on contracting parties. However, the theory that private law concerns corrective justice has

[91] Weinrib, 'Corrective Justice in a Nutshell' (n 13) 349.
[92] Weinrib, *Corrective Justice* (n 8) 21.
[93] Peter Benson, 'The Idea of Consideration' (2011) 61 University of Toronto Law Journal 241, 246.
[94] The intelligibility point relates to the rule of law wherein law exists in its own right without influence by other disciplines such as politics, sociology, or history. For a brief account of Weinrib's argument, see See Leslie Green, 'Law's Rule' (1986) 24 Osgoode Hall Law Journal 1023, 1027.

been challenged on multiple occasions by theorists who have argued that it may also be used for instrumental purposes. In their view, private law no longer exists to just '*be* private law'.[95] Instead, they say that private law may be understood as a means to achieve some independently justifiable goals. Those goals may be motivated by economics, politics, or morals, among other potential factors.[96] For example, the law-and-economics school of thought has had a significant influence on contract law scholarship. Private law is treated as a regulatory project of the state in which efficiency is prioritised. Ideally, contract law is developed to maximise the parties' wealth and therefore that of society generally.[97] The emphasis is placed on the function of the law, while form assumes a subordinate role.

However, the law and economics perspective does not encapsulate the essence of contract law. This is because it ignores the direct connection between the plaintiff and defendant which constitutes the private law relationship by prioritising the interests of the general community.[98] Contract law consequently becomes a mode of public regulation and diminishes private law's distinctive character. Moreover, it is less likely to create private law relationships that are intrinsically unified because it turns on independently justifiable goals.[99]

Therefore, the alternative theoretical accounts of contract law suffer from a 'line of doctrinal and structural shortcoming[s]'.[100] Structurally, they are not representative of the private law relationship as a unity between a particular plaintiff and defendant. The next issue is that of doctrine. If we are to examine smart contracts from a perspective that regards private law as internally intelligible, we must take seriously its cases, principles, doctrines, and standards.[101]

---

[95] To adopt the words of Weinrib. See Weinrib, *Idea* (n 14) 5.
[96] Dan Priel, 'Structure, Function, and Tort Law' (2020) 13 Journal of Tort Law 31, 17.
[97] Jonathan Morgan, *Contract Law Minimalism: A Formalist Restatement of Commercial Contract Law* (Cambridge University Press 2013) 43.
[98] Weinrib, *Idea* (n 14) 49.
[99] ibid.
[100] Benjamin Zipursky, 'Philosophy of Private Law' in Jules Coleman and Scott Shapiro (eds), *The Oxford Handbook of Jurisprudence and Philosophy of Law* (Oxford University Press 2002) 627.
[101] Weinrib, *Idea* (n 14) 9.

This thesis will map smart contracts to these components of contract law 'because an exposition that ignores them or does them violence runs the risk of being regarded as contrived or artificial or somehow amiss'.[102]

2.3 Coherence of contract law

Coherence is a fundamental principle of contract law and legal reasoning.[103] The need for coherence is not extinguished simply because established law is being applied to issues created by novel technologies.[104] Nor is a coherent approach to smart contracts impossible because contract law contains the necessary components to certain types of algorithmic contract, including smart contracts. However, some limits of legal coherence may be highlighted by smart contracts' technical characteristics including their immutability and lack of human comprehendible text. The courts may have difficulty reconciling the black-letter law and smart contracts which are too distinct from a regular fiat contract.

At its most basic level, coherence requires consistency in the law.[105] It is this consistency which ensures the intelligibility of the law. Thus, if a court's decision in a case is inconsistent with the existing body of principles, rules, and standards of contract law, then that decision lacks coherence. However, coherence understood more strictly requires that contract law is unified by a particular principle of the law; whether this principle is directed at the promotion of efficiency or the enforcement of promises, or some other goal.[106] In the framework which I have so far constructed, the underlying principle is the protection and enforcement of the rights and duties to which both parties have mutually assented.

---

[102] ibid.
[103] Weinrib, *Idea* (n 14) 38–42.
[104] Lauren Henry Scholz, 'Algorithmic Contracts' (2017) 20 Stanford Technology Law Review 128, 136.
[105] Smith (n 46) 11.
[106] ibid 12.

In so protecting and enforcing the rights and duties of the parties, the need for coherence further emphasises the connection between the plaintiff and the defendant in a private law relationship.[107] Without this connection, contract law would be less intelligible. This relationship is evident in the adjudicative process, doctrinal structure and remedial nature of contract law. In essence, the plaintiff brings a claim against a specific defendant. The claim is made based on certain contract law doctrines ranging from those governing formation to those which address the vitiation and enforcement of the contract. In analysing the dispute, the courts are primarily concerned with whether the parties' contract satisfies the rules of formation and whether it was made free from any mistakes, misapprehensions or breaches by one or both parties. It is less concerned with external factors, including parties who exist beyond the scope of a particular transaction, or addressing concerns of which the existing contract doctrines are not concerned.

At this point, it might be necessary to defend a potential objection regarding the conceptual framework proposed in this chapter, namely that the requirement of coherence in the law will result in the law's stagnation.[108] If the law is not sufficiently dynamic, it will not be able to adapt to account for novel technologies and how they might affect contracting practices. Hence, Guihot argues that 'new technologies create novel issues that press at the extremes of the established laws' and that the law is burdened by the requirement of coherence, and thus it is 'too slow to respond in time or with adequate answers'.[109] This is a valid concern, which is why the law may have to adapt in response to technological adaptations if necessary, while maintaining its coherence. Fortunately, the coherence of the corrective justice approach does not constrain the development of legal doctrine. This is because the coherence with which

[107] Weinrib, *Idea* (n 14) 43.
[108] On the claim that coherence results in legal conservatism, see Amalia Amaya, *The Tapestry of Reason: An Inquiry into the Nature of Coherence and Its Role in Legal Argument* (Bloomsbury Publishing Plc 2015) 58.
[109] Michael Guihot, 'Coherence in Technology Law' (2019) 11 Law, Innovation & Technology 311, 323.

corrective justice is concerned does not necessitate that 'later doctrine should conform to earlier doctrine'.[110] Instead, the corrective justice framework holds that earlier doctrine must change if it no longer reflects the private law relationship.[111] The risk involved with smart contracts is that they may disrupt the private law relationship, and existing doctrine may fail to reflect this.

However, it is argued that private law is sufficiently reflexive to account for most (but not all) blockchain transactions.[112] In a general sense, formalism involves the application by the courts of legal rules and doctrines of contract law according to their 'settled doctrinal construction' without regard for the instrumental purposes of contract law.[113] Such adaptation has already occurred within the realm of crypto-asset disputes in *AA v Persons Unknown*, however the decision in that case was based on instrumentalist reasoning.[114] The Court in that case prioritised the novel technology of cryptocurrency and adapted the law accordingly rather than foregrounding the legal concepts that constitute the body of private law (i.e. property law in that case).

In that case, a client of the plaintiff insurance company was subjected to a ransomware attack by the defendant, and as a result, the client's computer system was fully encrypted. The system was therefore accessible only by using the decryption tool, which the defendant claimed they would provide if they received US$1,200,000 in the Bitcoin cryptocurrency. The plaintiff insurance company thus paid the ransom and subsequently sought a proprietary injunction against the defendant. Before an injunction could be granted, the Court had to determine whether Bitcoin constituted a form of property. In so doing, the Court demonstrated how

[110] Weinrib, *Reciprocal Freedom* (n 33) 13.
[111] ibid.
[112] Larry A Dimatteo and Cristina Poncibó, 'Quandary of Smart Contracts and Remedies: The Role of Contract Law and Self-Help Remedies' (2018) 26 European Review of Private Law 810.
[113] Felipe Jimenez, 'A Formalist Theory of Contract Law Adjudication' (2020) 2020 Utah Law Review 1121, 1124.
[114] *AA v Persons Unknown* [2019] EWHC 3556 (Comm).

flexible the common law could be in response to crypto-assets.[115] This is because traditionally, the courts fit property into two categories: *choses* in possession or *choses* in action. Bitcoin constitutes neither of these categories because it is not physically possessable as required in the former category, nor are they an actionable right as required in the latter.[116] Instead, the Court applied the definition of property set out in *National Provincial Bank v Ainsworth* and found that Bitcoin adhered to that definition as it was sufficiently 'definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence'.[117]

While the decision in *AA* shows demonstrates adaptability of legal doctrine to crypto-assets, it is also an example of legal incoherence. The appellate courts have long regarded property as either choses in possession or choses in action, and the Court in *AA* effectively abandoned the dichotomy of property categorisation established across three centuries by the courts.[118]

One reason for this may be that crypto-assets are neither because they are pieces of information.[119] If they are merely information, crypto-assets are neither tangible objects that may constitute choses in possession, nor do they involve a legal right or claim, and therefore are not choses in action either. The reasoning applied by the Court in that case was instrumentalist because it adopted a category of property which did not have much judicial support in earlier appellate decisions. The reason for this decision may be that time was of the essence, and therefore *AA* was hastily decided to prevent the further dissipation of the plaintiff's assets.[120] If the decision was rendered quickly in this way, then the Court could not review the

[115] Rónán R Condon, '"BIT-PROPERTY"' (2020) 79 Cambridge Law Journal 224, 227.
[116] ibid 224.
[117] *National Provincial Bank v Ainsworth* [1965] AC 1175.
[118] Kelvin FK Low, 'Third Thing or Sixth Sense? I See Ideational Objects?' (Social Science Research Network, 31 January 2024) 2–3 <https://papers.ssrn.com/abstract=4716555> accessed 24 January 2025.
[119] Robert Stevens, 'Crypto Is Not Property' (2023) 139 Law Quarterly Review 621.
[120] Man Yip, 'Mareva Injunction and Crypto Fraud' in Hans Tijo and Paul S Davies (eds), *Fraud and Risk in Commercial Law* (Bloomsbury Publishing 2024) 123, 132.

matter in any great detail due to the time constraints placed on it. These constraints led it to reason instrumentally to provide the plaintiff with a provisional remedy. However, it would be more coherent to regard crypto assets as choses in action as they are, nevertheless, a form of intangible property.[121]

The courts need not introduce incoherent and unnecessary rules to accommodate smart contract transactions. Formalism is technology neutral and has the capacity to address new technologies without resorting to instrumental reasoning. For instance, in *Entores v Miles Far East Corporation*, the parties used a Telex to communicate the offer and acceptance of a contract.[122] The Court did not create a new doctrine to accommodate 'Telex contracts' but instead re-examined the postal rule in light of technologically facilitated modes of instantaneous communication. It found that the postal rule did not apply because the postal rule was better suited to long-distance communication. Instantaneous communication was held to be exempt from the postal rule, and acceptance was valid upon the receipt of acceptance by the offeree. Lord Denning reckoned with long-distance communications of acceptance, and in doing so, provided an analogy to shouting across a river.[123] He stated that, if the process was interrupted by an airplane flying overhead, the offeree would have to wait until the airplane had gone before they attempted to accept the offer again. Technologically, interruptions materialise in the form of the line going 'dead'.[124] The Court found the correlative connection in the form of their offer and acceptance of the parties notwithstanding that the contract was formed using the Telex. In a similar vein, contract law may be examined to determine whether the juridical relationship arises in the three different forms of smart contract: the bilateral smart contract which has no natural language document; the DASC; and the DAO smart contract.

[121] Kelvin FK Low, 'Bitcoins as Property: Welcome Clarity?' (2020) 136 Law Quarterly Review 345, 349.
[122] *Entores v Miles Far East Corporation* (1955) 2 QB 327.
[123] ibid 332.
[124] ibid.

D'Aloia v Persons Unknown is one example of a coherent decision regarding smart contract transactions.[125] A coherent decision centres on the direct connection between the plaintiff and defendant.[126] In *D'Aloia*, the plaintiff's claim initially involved seven defendants. The first defendant, persons unknown, had allegedly defrauded the plaintiff. The second defendant was Binance, a well-known cryptocurrency exchange with whom the plaintiff has settled. The fifth defendant was Aux Cayes, a crypto-wallet facilitator, against whom the plaintiff's claim was struck out by the Court.[127] The third and fourth defendants are also crypto-wallet facilitators against whom the plaintiff still seeks summary judgment in a separate application. It was the sixth defendant concerned in the particular judgment that has been handed down at the time of writing. The plaintiff claimed that some of his cryptocurrency was transferred to a crypto-wallet facilitated by the sixth defendant, 'Bitkub'. As such, one aspect of his claim was that Bitkub had been unjustly enriched because of the transfer from the first defendant's wallet to the wallet stored under Bitkub.

The Court found that there had been unjust enrichment because of the unauthorised transfers of the plaintiff's cryptocurrencies to the primary defendant's wallet and because the plaintiff had parted with those cryptocurrencies because of the primary defendant's fraud. However, the Court held that Bitkub had not been enriched at the expense of the plaintiff because he had not established that his cryptocurrency had reached the main defendant's wallet.[128] Consequently, Bitkub (in its capacity as a cryptocurrency exchange) was not liable to make restitution to reverse the alleged unjust enrichment.

To hold Bitkub liable in this instance would be incoherent. Corrective justice centres on the unified relationship of the parties in a transaction because they must be correlatively situated

[125] *D'Aloia v Persons Unknown* [2025] 1 WLR 821.
[126] Weinrib, *Idea* (n 14) 43.
[127] The reason being that the cryptocurrency could not be traced to a crypto-wallet facilitated by Aux Cayes. See *D'Aloia v Persons Unknown* (n 105) [262].
[128] ibid 8.

to one another.[129] This correlativity is identified through the transfer of value in the form of a bilateral transaction where 'one person gives and the other person receives something for nothing'.[130] There was no bilateral transaction between D'Aloia and Bitkub because D'Aloia failed to establish that Bitkub had been enriched at his expense as the cryptocurrency did not reach any wallet operated by Bitkub. Unless the defendant was enriched at the expense of the plaintiff, there may be no liability.[131] Unfortunately for D'Aloia, there was no causal factor to render a nexus between him and the exchange.

However, D'Aloia may coherently sustain an action against the first defendants who were in fact responsible for deceiving him and appropriating his cryptocurrencies. They had set up a website with a view to entice people to invest their cryptocurrencies into a fraudulent scheme. Through the website, they received something for nothing from the plaintiff. The transfer of value in this instance may render a direct nexus between them, a connection which was absent in the interaction between D'Aloia and Bitkub. Unlike in *AA*, *D'Aloia* was decided in a technologically neutral manner, focusing instead on whether there was a connection between the plaintiff and the defendant according to the existing law of unjust enrichment. The Court did not invent new reasoning to hold the cryptocurrency wallet operators liable simply to facilitate the novel technology, and instead adhered to the structure of the law, and consequently, corrective justice. The approach taken in in *D'Aloia* may serve as a lesson for the courts when deciding on a smart contract dispute in the realm of contract law also. That lesson is that the parties ought to be correlatively linked by factors intrinsic to the parties' relationship rather than arbitrary external considerations.[132] I will now turn to the requirement of correlativity, an element that is central to corrective justice, and therefore the law of contract.

[129] Weinrib, 'The Corrective Justice of Liability for Unjust Enrichment' (n 29) 170.
[130] ibid 172.
[131] ibid.
[132] Weinrib, *Idea* (n 14) 39.

2.4 Correlativity

2.4.1 Gains and losses

I have already mentioned correlativity in the preceding sections, but it is worth developing an a further understanding of it because it is through the correlativity of the parties' interaction that the fairness of the transaction is figured. Under a corrective justice approach to private law transactions, one party must have made a gain that is correlative to the loss made by his contracting counterpart in order to attract liability.[133] However, private law gains and losses can be further divided into those which are factual and those which are normative.[134] A party can make a factual gain which corresponds to the other party's factual loss and may not be held liable under the contract. This is because a factual gain or loss alone is insufficient to render a party liable. Therefore, it is essential that there exists some normative gain or loss in the interaction between the plaintiff and defendant.

Before I identify specific smart contract examples of factual and normative gains and losses, it is necessary to state the difference between these two concepts. A factual gain is assessed with regard to the holdings of the contracting parties. Thus, a party obtains a factual gain when his holdings have increased and makes a factual loss when his holdings have decreased.[135] Thus, factual gain and loss can be quantified in terms of material or economic gain or loss. In contrast, whether a party has realised a normative gain or loss is determined according to the legal norms which apply to the facts of a particular dispute. These norms are the tools which the courts can use to determine whether or not a transaction was fair.[136] This is achieved by identifying any

[133] Ernest J Weinrib, *The Idea of Private Law* (Oxford University Press 2012) 114.
[134] ibid.
[135] Weinrib, *Idea* (n 14) 116.
[136] ibid 115.

discrepancies in the transaction between the holdings of the parties following the transaction against those holdings which the parties *should* have post-transaction.

The distinction between factual and normative gains and losses is demonstrated in *Hadley v Baxendale*.[137] The claimants in that case were millers whose business suffered as a consequence of a broken machine at their mill. To repair the equipment, the plaintiffs contracted with the defendant to deliver the broken component of the machine to some repairers. The defendant failed to deliver the item by the agreed upon date and therefore the business remained out of operation. This is an example of a factual loss because the plaintiffs lost business and thus lost profits. Yet, the plaintiffs were unsuccessful in their attempt to recover the lost earnings because there was no normative loss. There was no discrepancy according to the norms which governed the parties' interaction such that the defendant could be held liable for Hadley's losses. The governing rule here was breach of contract which was assessed according to the norm of foreseeability. Thus, the question raised by Alderson B. was whether the damages were sufficiently foreseeable by the defendant to bar a claim for damages, to which the court concluded they were not. As such, there was a factual loss realised by Hadley. Notwithstanding the factual loss, there was a lack of a normative loss sufficient to ground the plaintiff's claim.

Smart contract transactions may also involve losses which are distinctly factual or normative. For instance, a party may receive a crypto-asset via an 'airdrop'. Airdrops are used by crypto-asset projects as a method to promote their project by distributing free tokens among a cohort of users. There are numerous ways in which a user may receive an airdropped token, but for the present purpose to demonstrate the point, I will focus on 'exclusive airdrops' where the user is selected based on criteria set out by the project's development team. Candidates for the airdrop may therefore be chosen according to their influence within cryptocurrency circles,

[137] *Hadley v Baxendale* (1854) 156 ER 145.

their expertise, or their contribution to the project.[138] The developers may attempt to provide an airdrop to a hypothetical Michael Thompson because he is a well-known advocate for the blockchain and cryptocurrency markets. If they enter the incorrect crypto-wallet number into the smart contract, they may address the airdrop to the wrong individual. Without the recipient's co-operation, it may be difficult to retrieve the token. Moreover, the project's developers may not be able to recover the token under contract law because the recipient owes them nothing. This is because although the recipient received a factual gain (according to the token's value), it was not a normative gain.[139]

Through the need for normative gains and losses, corrective justice limits the instances of recovery to where the right of one party has been infringed. Thus, a harmed party will not always be able to recover notwithstanding his losses. Making this limitation explicit is necessary to quell claims that most on-chain transactions will be recoverable simply because they resulted in loss to one party. Instead, recovery is limited to smart contract transactions in which a normative gain corresponds to a normative loss according to the rights and duties of the contracting parties.

2.4.2 Bilateral structure of right and duty

The correlative concepts of right and duty indicate instances where liability will, or should, arise. Ideally, a defendant will be held liable where his actions are incompatible with the right of the plaintiff.[140] Thus, the right and duty involved in the contract law relationship are also

[138] What Is a Crypto Airdrop?' <https://www.coinbase.com/learn/crypto-basics/what-is-a-crypto-airdrop> accessed 4 March 2025.

[139] This hypothetical scenario develops Weinrib's example making the same point but in a manner that applies it to smart contracts: 'if another mistakenly paves my driveway without my knowledge, the condition of my holdings is improved, but I owe the improver nothing'. See Ernest J Weinrib, *The Idea of Private Law* (Oxford University Press 2012) 116.

[140] Weinrib, *Reciprocal Freedom* (n 33) 26.

correlatively structured. Given the correlativity of right and duty, it follows that the parties are viewed in a unified manner as 'interactors', therefore the welfare or interests of one party or the other may not be considered in isolation.[141] Instead, the transaction is viewed in its totality.

Specifically, the right with which this thesis is concerned is the right to contractual performance in the way which the parties had intended. The parties to a contract establish this right when they express their mutual consent to be bound by the contract.[142] Once the contractual right between one another has been established, the plaintiff has a right with which the defendant has a duty not to interfere. The function of the contract thus is to enact a 'voluntarily assumed change in the pre-existing legal relationship between the contracting parties'.[143] The right embodies the freedom of the plaintiff to contract upon any grounds which he deems appropriate for his needs as a 'free and purposive' agent.[144] It is this right which contract law ought to protect.

There is a risk that the bilateral structure of right and duty breaks down when smart contracts are used instead of traditional contracting methods. For example, Fairfield and Selvadurai state that a smart contract may create rights but not give rise to any corresponding obligations as traditionally understood within the law of contract.[145] This is because the rights that are established via a smart contract are automatically enforced by its code, therefore no duty arises on the defendant's part because he has no role to perform once the smart contract has been executed. In other words, he has no obligations to the plaintiff, strictly speaking, because these are mechanised by the smart contract. However, this argument is based on the idea that smart

[141] ibid 28.
[142] ibid 29; Barnett has proposed a well-known theory which identifies consent as the fundamental requirement of contracting. However, Barnett's theory can be distinguished from Weinrib's because the latter sees contract law as an end in itself, while the former views it as a means of transferring entitlements. See Barnett (n 6).
[143] Ernest J Weinrib, 'Punishment and Disgorgement as Contract Remedies Symposium: Private Law, Punishment, and Disgorgement' (2003) 78 Chicago-Kent Law Review 55, 66–67.
[144] Weinrib, *Idea* (n 14) 123.
[145] Joshua Fairfield and Niloufer Selvadurai, 'Governing the Interface between Natural and Formal Language in Smart Contracts Special Issue: Governing the Digital Space' (2022) 27 UCLA Journal of Law and Technology 79, 105–106.

contracts will mostly ensure *perfect performance.* Although perfect performance is the ideal for which smart contract developers should strive, it may be difficult to achieve in practice because coding errors and malfunctions are statistically likely to occur in any software, including smart contracts.[146] Glitches in contracting software have already resulted in claims of breach of contract.[147] Therefore, it remains necessary to ascertain the duties and obligations of the defendant in a smart contract transaction because the smart contract may not successfully enforce the plaintiff's rights on its own.

2.5 The regulatory-instrumentalist discussion versus the ongoing need for private law

Regulatory-instrumentalism is one of the avenues through which functionalists may achieve specified objectives. It is worth setting out the regulatory-instrumentalist position briefly before concluding this chapter because much of the discussion on smart contracts have taken the form of regulatory-instrumentalism.[148] Such a public law, regulatory response is justified insofar as blockchain technology threatens the rule of law and the wellbeing of society broadly.[149] Thus, public law may be used to regulate instances where the blockchain is used by entities for nefarious purposes such as widescale fraud, the sale of drugs and firearms, money laundering, and terrorism-financing, among others.[150] For instance, heightened regulatory oversight was desirable following the collapse of the 'FTX' cryptocurrency marketplace wherein retail

[146] Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (2017) 9 Law, Innovation & Technology 269, 281.
[147] Ghodoosi (n 7) 81; *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC (I) 03.
[148] Roger Brownsword, 'Smart Contracts: Coding the Transaction, Decoding the Legal Debates' in Philipp Hacker and others (eds), *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019) 317; Primavera de Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018); Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press 2018).
[149] Yeung (n 48) 8.
[150] The blockchain is undoubtedly a useful tool for criminals. See Chainalysis Team, '2024 Crypto Money Laundering Report' (*Chainalysis*, 15 February 2024) <https://www.chainalysis.com/blog/2024-crypto-money-laundering/> accessed 10 December 2024; See also 'Silk Road: The Dark Side of Cryptocurrency' (21 February 2018) <https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/> accessed 10 December 2024.

investors and institutions suffered significant losses.[151] However, the need for some public law regulation does not override the need for private law remedies because smart contracts are ultimately about interpersonal transactions. If the plaintiff has a right to which the defendant has a correlative duty, a contract law remedy may vindicate the plaintiff's right if it was infringed by the defendant.[152] Corrective justice through contract law is concerned with the 'doing and suffering' by bipolarly situated parties.

Brownsword argues that the instrumentalist approach is required in response to new technologies because it identifies specific regulatory objectives and uses the law as a means to achieve them.[153] In this regard, the regulatory-instrumentalist would argue that new technologies warrant bespoke laws and that regulatory-instrumentalism is the best way to achieve this. Similarly to functionalism, regulatory-instrumentalism seeks to achieve certain predetermined goals. One possible objective of the regulatory-instrumentalist approach is the *ex ante* management of risk while other objectives include the use of law as a means to further economic objectives. Another might be the increased competitiveness of the legal system of a particular jurisdiction if it has a suitable governance regime for smart contracts in place. Although the UK Law Commission in its Report on smart contracts was skewed towards the coherentist mindset, it was also influenced by this instrumentalist concern for the general appeal of the UK legal system as a forum of choice for business.[154]

Having set out some of the overarching goals of regulatory-instrumentalism broadly, it is worth outlining some of instrumentalist approaches to smart contracts specifically. Some of these

[151] Jennifer J Schulp, 'Crypto Crash: Why the FTX Bubble Burst and the Harm to Consumers' (*Cato Institute*, 14 December 2022) <https://www.cato.org/testimony/crypto-crash-why-ftx-bubble-burst-harm-consumers> accessed 13 September 2024.
[152] Weinrib, *Corrective Justice* (n 8) 172.
[153] Roger Brownsword, *Law, Technology and Society: Re-Imagining the Regulatory Environment* (Routledge 2019) 194.
[154] UK Law Commission, 'Smart Legal Contracts: Advice to Government' (2021) Law Com No 401 20; Brownsword, 'Regulatory Fitness' (n 17) 17.

ideas stem from Lessig's thesis that cyberspace can be made regulatable by mandating changes to its architecture.[155] For instance, blockchains are highly reliant on code to operate, and therefore regulations can be directed at code designers that will determine how crypto-assets and smart contracts can be used. De Filippi and Wright suggest that laws could be established that mandate the inclusion of specific features in the blockchain architecture by software designers that give the government power to terminate smart contracts or other blockchain applications that are not legally compliant.[156] Furthermore, they suggest that developers could be incentivised to design applications carefully by holding them strictly liable for blockchain applications that result in damage. Instead of relying on litigation after the would-be plaintiff has suffered harm, regulators may try to prevent the harm from happening in the first place by rewarding the compliance of coders, or by terminating blockchain applications that would traditionally result in litigation. For example, software developers may have an increased role in ensuring that smart contracts that do not reflect the parties' intentions are not executed. Similarly, a smart contract that contains stolen cryptocurrency may be prevented by an agent who has been granted the ability to do so. The idea here is that private law remedies are replaceable by a new form of technological management of risk.

The most significant effort to regulate certain aspects of the blockchain to-date was made by the European Union through its enactment of the Markets in Crypto Assets Regulation 2023 (MiCAR). The Regulation aims to bolster users' confidence in their use of crypto-assets, safeguard against 'regulatory fragmentation', and the mitigation of risk.[157] This is primarily achieved by imposing strict obligations on crypto-asset service providers (CASPs). For instance, they must be authorised by a central body like the Central Bank, and must have a crisis management plan in place. The approach adopted by the EU in its response to crypto-

[155] Lawrence Lessig, *Code 2.0: And Other Laws of Cyberspace* (Basic Books 2006) 67-68.
[156] de Filippi and Wright (n 148) 181.
[157] Regulation on Markets in Crypto-Assets 2023 Preamble, ss 4-5.

assets is broadly in line with instrumentalist thinking of De Filippi and Wright. For instance, they suggest firstly that governments can directly regulate end-users of blockchain applications.[158] Although this comes with its own practical challenges due to the decentralised and pseudonymous nature of the blockchain, they suggest that this can be overcome through sophisticated technological solutions such as big data analysis, and by tracking transactions so that users can eventually be identified. Nevertheless, they accept that it is too burdensome a task to regulate the end-user and suggest that the focus of regulators could instead be placed on the blockchain-based intermediaries. Centralised operators who control access to network of a particular blockchain can be required to follow a large set of laws, such as the need to police undesired behaviour and to disallow certain transactions that would be prohibited by the law.[159] In essence, this is what MiCAR does, by placing anti-money laundering requirements on CASPs and requiring them to prevent market abuse.

While such public law regulation directed at gatekeepers of the crypto-economy is a necessary response to protect crypto-asset consumers, it is less concerned about the peer-to-peer or business-to-business contractual relationships that may be established via the blockchain. Instead, it is directed at ensuring financial stability in regards to the crypto-economy more broadly. This means that private law, in the form of contract law, is still necessary to govern those relationships created by parties using smart contracts.

Moreover, a reason to assess smart contracts using a private law specific paradigm is because smart contracts are naturally the subject of private law. Private law is concerned with the bilateral relationship established between two contracting parties. For our purposes which centre particularly on contract law, private law concerns the connection between horizontal relationship between two parties who enter into non-gratuitous, and commercial, transactions.

[158] de Filippi and Wright (n 148) 175.
[159] ibid 179.

The vertical relationship between an individual and the state is not the concern of private law.[160] The role of the state exists insofar as it sets out standards which must be met in order for a contract to be valid, but ultimately the contract which the parties create is binding specifically on those parties and sets out their obligations toward one another.[161]

Smart contracts therefore exist primarily within the domain of contract law. They are often created between two parties, typically with a view to exchange a crypto-asset. While various methods of smart contract usage exist, a routine transaction would take place as follows. Party B seeks to trade his Ethereum cryptocurrency for Party A's Solana cryptocurrency. Party A is willing to trade her Solana at its market rate, but seeks that Party B must pay the gas fees for the transaction in addition to the Ethereum.[162] As such, Party A will code the smart contract and place her Solana into the escrow of the smart contract. She will also write any other agreed upon terms into machine-readable code so that it can be executed by the smart contract. This includes the gas fee, which fluctuates according to the amount of network traffic at the time of the transaction. Thus, if there is significant congestion on the network, the fee will be higher. Party A might account for the fluctuation by coding a term to the effect that '*if* network traffic is high, Party B must pay >10% gas fee'. The rights, duties, and obligations of the parties are primarily contained in the smart contract and they exist solely between the two parties. They do not invoke the state's authority over the agreement.[163]

Even where a decentralised cryptocurrency exchange is involved, the transaction still takes place between the two transacting parties because the decentralised exchange does not exist to

[160] Ernest J Weinrib, *The Idea of Private Law* (Oxford University Press 2012) 8.

[161] Michael Da Silva, 'Formalising Formalism: Weinrib, Aristotle, and the Nature of Private Law' (2018) 9(3) Jurisprudence 486, 487.

[162] Gas fees are an important part of the Ethereum blockchain which users must pay to execute transactions on the blockchain. See 'What Are Gas Fees?' <https://www.coinbase.com/en-gb/learn/crypto-basics/what-are-gas-fees> accessed 3 March 2025.

[163] Certain exceptions exist here including smart contracts entered into by minors and those which fall under the category of illegal contracts.

intermediate the transaction.[164] Instead, it acts as the virtual marketplace where two parties submit their buy and sell orders using their smart contracts independently of the exchange. In essence, the transaction is to be treated as though two parties met at a public square and bargained with one another there. In other words, the transaction is considered peer-to-peer rather than peer-intermediary-peer.

2.6 Conclusion

This chapter has outlined the theoretical framework through which smart contract transactions will be analysed throughout this thesis. Specifically, the framework draws upon the concept of corrective justice as influentially discussed by Ernest Weinrib as the key regulative feature of the private law transaction. Thus, a legal formalist approach encompassing the corrective justice principle is adopted, to ascertain the extent to which contract law is prepared in its response to smart contract based disputes. Despite their technological characteristics, including immutability, pseudonymity, and code-based execution, smart contracts fundamentally remain as instruments of the private law transaction that should be subjected to the principles concerning contract formation through to vitiation, and ultimately, the remedies that flow from the private law adjudicative process.

The corrective justice framework adopted emphasises the bilateral structure of the private law relationship, including the rights and duties of the parties. Although smart contracts may appear to automate performance and therefore eliminate any clear duties of the promisor, the potential for coding errors, malfunctions or deliberate breaches means that understanding the correlative rights and duties of contracting parties remains essential. Thus, when a party suffers a

[164] Cryptocurrency Exchange Architecture: Building a Secure and Scalable System' (*Debutinfotech*) <https://www.debutinfotech.com/blog/cryptocurrency-exchange-architecture> accessed 13 January 2025.

normative loss through a smart contract transaction, contract law may provide the necessary remedy in order to restore balance between the parties.

Historically, the courts have proved themselves to be adept at adapting contract law in response to 'new' technologies without requiring radical legal reform. From vending machines, to telephones, to click-wrap agreements on the internet, the courts will similarly be able to map the elements of the smart contract transaction to various established doctrines in the law of contract. Technological innovation will only affect the application of contract law once the smart contract transaction becomes so complicated that it no longer looks like a contract transaction. Thus, it is unlikely that the requirement of coherence should bar the law from adapting to smart contracts if necessary.

Although regulatory-instrumentalist approaches like that adopted by the EU in the *Markets in Crypto-Assets Regulation 2023* address important public law concerns surrounding blockchain technology, they do not account for the private law relationship established between smart contracting parties. The horizontal relationship between two parties who enter into non-gratuitous transactions remains the subject of contract law, regardless as to whether those transactions are executed using traditional or smart contracts.

Thus, in conclusion, while smart contracts present unique challenges to traditional contract law principles, the formalist framework centred on corrective justice is the most suitable for assessing contract law's fit with smart contracts. In carrying out this analytical exercise, the correlative rights and duties of the parties and the coherent application of contract law's doctrines and principles must be emphasised. Anything else may stray from the overall objective of this thesis: to examine smart contracts through a 'pure' contract law lens.

3 From Paper to Digital Agreements: The Formation of Smart Contracts

3.1 Introduction

The contract formation process embodies corrective justice. The offeree's entitlement to the offeror's performance is determined during the contract's formative stages. Although they are temporally separated, the offer and acceptance of a contract constitutes a single, uninterrupted chain which binds the parties together.[165] These two acts, by the offeror and offeree respectively, must be disconnected in this way because two concurrent offers are not binding, and therefore do not create a unified relationship between the parties.[166] A contract is not validly formed where one of these components exists without the other. The substantive content of the parties' agreement derives from the initial offer. Therefore, the doctrines of offer and acceptance are significant from a corrective justice standpoint because they determine how the parties' standing in relation to one another are modified. Once the plaintiff's right is established under the contract, the defendant has a duty to not interfere with it. However, the offeree must have provided some consideration in return for the promise, otherwise the contract will not be binding. In that sense, the doctrine of consideration captures the reciprocal nature of the juridical relationship because it ensures the offeree's participation in establishing his right to the offeror's performance.[167] Consideration is, ultimately, a 'token of the will' of the parties to engage as 'equal agents' in the transaction.[168] Without it, the bilateral connection between the parties cannot be created.[169]

It is essential under corrective justice that the parties are linked by the transaction. Therefore, a smart contract may not be identified as a contract if it is incapable of containing an

[165] Ernest J Weinrib, *The Idea of Private Law* (Oxford University Press 2012) 137.
[166] ibid; Where there are concurrent offers, the second offer in the sequence is treated as a counter-offer which 'kills the original offer'. See *Trollope & Colls Ltd v Atomic Power Constructions Ltd* [1963] 1 WLR 333, 337.
[167] Weinrib, *Idea* (n 14) 138.
[168] Weinrib, *The Idea of Private Law* (n 18) 138.
[169] Benson, 'The Idea of Consideration' (n 57) 251.

intelligible offer. Although an offer may be expressed in many different forms including computer code, the offeree must be able to unequivocally accept its terms. The requirement of unequivocalness presupposes that the offeree has understood the offer enough so as to accept it. However, computer code is used to instruct a computer to perform and may evade a human party's ability to comprehend its terms.[170] If an offeree cannot understand the terms advanced in computer code form, then his ability as an equal agent to self-determine may be impeded. If this is the case, a smart contract may not be a contract at all. Such a finding stands in contrast to the existing literature, in which some scholars hold that smart contracts may readily be declared as legally binding contracts. Scholars such as DiMatteo and Cannarsa, and Rohr, state that smart contracts could be enforceable where the courts equate them to written contracts, or where the parties have assented to the use of code.[171] However, it is argued that corrective justice precludes such smart contracts from constituting enforceable contracts in this way because code alone involves the vagaries of the parties' private intention, to which contract law 'cannot be held hostage'.[172] Due to the vagaries involved in DASCs and DAOs, the actions of one's computer code or algorithm may not coexist with the other party's freedom. Consequently, the smart contract may not constitute a legal contract where it is not combined with a natural language component. As such, parties who use DASCs and DAOs and suffer normative losses may have to look beyond the law of contract for a remedy.[173] Moreover, this chapter provides an in-depth analysis of DAO smart

[170] Eliza Mik, 'Contracts in Code?' (2021) 13 Law, Innovation & Technology 478, 483.
[171] For example, see Larry A DiMatteo, Michel Cannarsa and Cristina Poncibò, 'Smart Contracts and Contract Law' in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019) 9; and see Jonathan G Rohr, 'Smart Contracts and Traditional Contract Law, or: The Law of the Vending Machine' (2019) 67 Cleveland State Law Review 71, 85.
[172] Weinrib, *The Idea of Private Law* (n 18) 104.
[173] The alternative course of action proposed by this thesis is found in the form of unjust enrichment. See Chapter 7 for discussion on how the law of unjust enrichment resolves smart contract related disputes involving code-only agreements.

contracting, which appears to have evaded detailed scholarly attention from a contract law perspective.

Nevertheless, the doctrine of consideration will often be satisfied in a smart contracting context because a smart contract cannot be executed without the submission of some 'token of the will' by the offeree. Specifically, this 'token' will take the form of a cryptocurrency or other crypto-asset, like the Ether cryptocurrency. The code of the smart contract may stipulate the required price for the exchange. If the offeree fails to pay this price, the smart contract will not execute.

Smart contracts are a new technology that change the way parties conduct transactions, and which have the potential to replace contract law as the primary mode of governance for these transactions.[174] They are pieces of software which automate the performance of parties' agreements, and which may express their rights and duties in the form of code.[175] This definition has led to some tension as to how smart contracts should be classified according to contract law. On the one hand, they are merely a bunch of code like other forms of software, and therefore carry no legal significance.[176] On this view, code cannot create legal obligations between parties. On the other hand, a smart contract expressed entirely in code may constitute a legally binding agreement.[177] Smart contracts, through a 'formal language' (i.e. code) embody the very rights and duties which are the concern of contract law. It is therefore necessary to examine the extent to which these 'agreements' map on to the doctrines of contract formation. As such, smart contracts must include adequate offer and acceptance, consideration, and an intention by their parties to create legal relations. If they fail to satisfy these requirements, then

[174] On this view, smart contracts displace contract law as they are self-enforcing, self-executing, and self-remedying and no longer require its intervention. *See* Cristina Poncibò and Larry A DiMatteo, 'Smart Contracts: Contractual and Noncontractual Remedies' in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019).
[175] Evripidis Rizos, 'A Contract Law Approach for the Treatment of Smart Contracts' "Bugs"' (2022) 30 European Review of Private Law 775, 790.
[176] Mik, 'The Sense and Nonsense of Smart Contracts' (n 5) 9.
[177] Allen (n 47) 329.

smart contracts may not result in the creation of *in personam* rights, without which a party cannot be said to have an obligation to perform for another.[178] Code-only smart contracts such as DASCs and those used in DAOs may not confer a performance right because they do not facilitate an offer that is comprehendible to the offeree.

This chapter begins by setting out the rulebook of contract formation typical of common law jurisdictions. It subsequently applies these doctrines to identify whether smart contracts can result in the creation of an enforceable right, or if they are simply software that cannot be enforced. But first, it identifies certain factors that will affect how smart contracts map onto the doctrines of formation (and other doctrines in later chapters). Then, in its evaluation of offer and acceptance within smart contracts, it contends that these components can be easily recognised in bilateral smart contracts where a plain language agreement precedes the coded 'contract.' There is, however, a slightly greater challenge in identifying an offer when it exists solely in coded form, but it is not impossible. The doctrine of consideration, it is argued, is not significantly challenged because smart contracts cannot be executed without the payment of the stipulated value of a chosen crypto-asset into them. However, tension arises around the intention to create legal relations between smart contracting parties. They may either view smart contracts as merely software for controlling certain crypto-assets, or they may believe that no liability should arise because they are interacting via decentralised methods.[179] Ultimately, it is argued in this chapter that some smart contracts will result in enforceable rights and in some cases, such rights, and their corresponding duties, may not be created.

[178] Weinrib, *Corrective Justice* (n 8) 189.
[179] Ilya Kokorin, 'The Decentralisation Defence' (2025) 57 Computer Law & Security Review 106148, 2.

3.2 Contract rulebook

In this section, I will discuss the rules regarding the formation of valid contracts by examining the formalities required under common law that determine whether an agreement is legally binding. I will then discuss the doctrines of contract law that apply when a contract has been vitiated. This thesis operates on the understanding that courts in common law jurisdictions tend to fit new technologies 'into the marked slots of offer, acceptance and consideration', as well as other long-established categories of contract law.[180] The courts will likely approach smart contracts in a similar manner, thus taking seriously these formative concepts.

3.2.1 Offer

An offer in a smart contract transaction is different to an offer in a traditional contract. This is because a smart contract offer is made in the form of software code that is posted to the blockchain rather than in plain language. Particularly where the smart contract is written only in code, contractual parties and courts may find it difficult to ascertain what the offer actually involves. Sometimes however, the code of the smart contract may be plainly defined in a separate document to the smart contract programme. If such a document exists, it will render the rights and duties of the smart contracting parties more intelligible for the courts and the parties themselves.[181]

An offeror must satisfy an objective test before their proposal may constitute a valid offer. An offer must consist of a definite statement of the terms on which the offeror is willing to contract and to which they intend to be bound if specific conditions are met.[182] The offer constitutes the

[180] Roger Brownsword, 'Regulatory Fitness: Fintech, Funny Money, and Smart Contracts' (2019) 20 European Business Organization Law Review 5, 16; *New Zealand Shipping Co Ltd v A.M. Satterthwaite & Co Ltd* [1974] 2 WLR 865, 167 (per Lord Wilberforce).
[181] Jeremy M Sklaroff, 'Smart Contracts And The Cost Of Inflexibility' (2017) 166 University of Pennsylvania Law Review 263, 275.
[182] Robert Clark, *Contract Law in Ireland* (Eight edition, Round Hall Thomson Reuters 2016) [1-08].

first stage of the bipolar relationship between the parties which ultimately leads to the voluntary and mutual assent of both parties to the unified transaction.[183] It is bipolar because an offer without acceptance cannot unite the parties in a single transaction.

To initiate the contracting process, there are four essential requirements to an effective offer which the promisor must satisfy. Firstly, there must be a communication of the terms of the offer. Secondly, the promisor must show a willingness to be bound by those terms. Thirdly, the offer forms a binding agreement only when certain conditions are met. Finally, the content of the offer must be definite. In this sense, the offeror's intention should be objectively clear from an appraisal of the offer. However, if the offer is only presented in software code via smart contract, the terms of the offer may be unclear to the offeree as analysing code remains a specialist skill.[184]

If an offer lacks the requisite clarity, the court may hold the offer to be a mere statement, an invitation to treat, or that it is void for uncertainty. Where a party uses language that evidences his hesitancy to commit to a contract, the courts will likely find there was no offer. For example, in *Gibson v Manchester City Council*, the House of Lords found that a party's statement that he 'may be prepared to sell' was not sufficiently certain to constitute a binding offer.[185] In Ireland, the Court in *Central Meats v Carney* held that a proposal to supply an unspecified quantity of cattle to a meat factory did not amount to an offer.[186] Additionally, the statement in that case did not outline the quality or the sale price of the meat to the offeree. Therefore, the

[183] Curtis Bridgeman, 'Corrective Justice in Contract Law: Is There a Case for Punitive Damages Note' (2003) 56 Vanderbilt Law Review 237, 252.
[184] Sarah Green, 'Smart Contracts, Interpretation and Rectification' (2018) Lloyd's Maritime and Commercial Law Quarterly 234, 241. See particularly footnote 31, in which Green notes that the outcome of particularly complex code may not be predicted even by proficient coders. In other words, it is hard to determine what the offer is until after the smart contract has been executed.
[185] *Gibson v Manchester City Council* [1979] 1 WLR 294, 298.
[186] *Central Meats v Carney* [1944] 10 Ir Jur Rep 34.

subject-matter of any offer - whether analogue or digital - must be sufficiently clear before the courts will recognise it as binding.

3.2.2 Invitation to treat

Typically, an advertisement for a product on a website is considered to be an invitation to treat. This rule safeguards sellers from liability when they have a limited amount of stock and therefore would be unable to fulfil all accepted offers.[187] Sellers are protected because contract law's own doctrines prevent them from over-accepting offers when the buyers' demand exceeds the sellers' supply. In *Grainger & Sons v Gough* for example, a wine merchant distributed a list of wines including their prices.[188] The plaintiff ordered wines from the list at the stated price, which the defendant refused to deliver. The House of Lords held that the price list was not an offer, but an invitation to treat, because the merchant's wine stock was limited. Had the list constituted an offer, the merchant would theoretically be open to an unlimited number of acceptances.

Overselling one's assets is less of an issue in real-world transactions where performance often requires the physical handing over of goods by the seller to the buyer. In online transactions however, liability would arise on a global scale if all online advertisements constituted offers. It is sensible therefore to limit the amount of obligations that arise out of online transactions.

It is clear from *Lefkowitz v Great Minneapolis Surplus Store* that an advertisement may be an offer rather than an invitation to treat if it is specific in outlining the content of the transaction, and leaves no room for negotiation.[189] In that case, the plaintiff sought to purchase a fur coat from the defendant having relied on an advertisement the latter had published stating it would

[187] Eliza Mik, 'Certainty at Last? A "New" Framework for Electronic Contracting in Singapore' (2013) 8 Journal of International Commercial Law & Technology 160, 171.
[188] *Grainger & Son v Gough (1896)* AC 325.
[189] *Lefkowitz v Great Minneapolis Surplus Store* (1957) 86 NW 2d 689.

be sold on a 'first come, first served' basis. The defendant refused to provide the coat to the plaintiff as a store rule stated that they would only sell to female customers. However, due to the specific language of the advertisement, the Court held that the advertisement was a valid offer.

Some smart contracts may not themselves be intended as an offer, and thus they may instead be an invitation to treat. An invitation to treat involves a willingness by a party to negotiate with others with a view to concluding a contract.[190] Among other things, goods displayed for sale, advertisements, and auctions constitute an invitation to treat rather than an offer. Thus, crypto asset transactions may also involve invitations to treat. For example, blockchain based transactions are often facilitated by intermediary marketplaces such as OpenSea.io or Nifty Gateway. These online marketplaces act as virtual shelves upon which prospective buyers can browse digital and crypto-assets.

3.2.3 Unilateral and bilateral contract distinction

Contract law has long recognised a difference between unilateral and bilateral contracts. This distinction is important as a smart contract offer may take the form of either a unilateral or bilateral contract and the applicable rules of contract law differ depending on the form of the contract.

A unilateral offer occurs where one party makes a promise to the other in exchange for a specified act.[191] Thus the offeree is entitled to the benefits of the contract once he has performed the required act. In other words, a unilateral offer operates on an 'if x, then y' basis. The classic example of a unilateral offer involves the provision of a reward for finding a person's lost pet.

[190] Ewan McKendrick, *Contract Law* (9th edn, Palgrave Macmillan 2011) 27.
[191] Hugh Collins, *The Law of Contract* (4th edn, Cambridge University Press 2003) 62.

The offer in that case is stated as 'if you find my dog, I will pay you €100'. This is how many smart contract transactions operate as the crypto asset is coded into the smart contract pending the acceptance by an offeree.[192] Such offers can be open to anyone who has access to the online crypto marketplace on which the smart contract has been submitted. Only the offeror is bound to a unilateral offer until a second party has accepted it.[193] In contrast, a bilateral contract involves mutual promises between two parties, and binds both parties at the same time. In such an arrangement, each party commits to fulfilling an obligation in return for the other's promise.

3.3 Acceptance

Once it has been established that a valid offer has been made, there must be a corresponding valid acceptance of that offer. Similarly to an offer, an acceptance requires an unequivocal expression of intention by the offeree to be bound to the terms of the agreement, and it must be communicated by the offeree. Following the objective approach used by the courts, a party may be bound to a contract if a reasonable person would believe he assented to the terms proposed by the offeror.[194] The doctrines of offer and acceptance taken together form the basis of the parties' integrated action, giving rise to the parties' correlative right and duty. The doctrines unite the two seemingly separate acts of offer and acceptance into one united sequence.[195] As Weinrib argues, neither a party's offer or the counterparty's acceptance has any juridical significance if they exist in isolation. An enforceable contract only comes into being once both of these elements are present.

The second principle of acceptance requires that the offeree communicates acceptance to the offeror. Lord Denning stated in *Entores Ltd v Miles Far East Corporation* that an offer is not

[192] Robert Herian, 'Smart Contracts: A Remedial Analysis' (2021) 30 Information & Communications Technology Law 17, 19.
[193] Paul Anthony McDermott, *Contract Law* (2nd edition., Bloomsbury Professional 2017) [2.26].
[194] *Smith v Hughes* (1871) LR 6 QB 597, 607
[195] Weinrib, *Idea* (n 14) 137.

accepted until the offeree has ensured the offeror has heard his acceptance.[196] However, communication is not necessary in unilateral contracts because acceptance in that context is signalled through performance. As will be discussed in the analysis section, this exception is a default rule in a unilateral smart contract because the performance of its terms are sufficient for its execution. In essence, once the stipulated amount of cryptocurrency (or Fiat currency if permitted) is paid into the smart contract, it will execute regardless as to who made the payment or whether they have communicated their desire to accept the contract.

3.4 Consideration

The third requirement for a legally binding agreement is consideration, without which a court may hold that a smart contract is not enforceable. The doctrine of consideration requires that the recipient of the promise transfers something of value in the eyes of the law. The doctrine plays an important role the contracting process as it confirms the parties' equality in the transaction, and shows that they both will to establish the contract.[197]

Lord Dunedin in *Dunlop v Selfridge* described consideration as 'the price for which the promise of the other is bought'.[198] In this regard, one party receives a benefit while the other suffers a detriment.[199] Without consideration, an agreement cannot be enforced by the courts as they may only enforce promises for which the promisee has given something in exchange. The doctrine aids the courts in determining whether an agreement is enforceable or whether they must look to other legal concepts to resolve the dispute.[200]

[196] *Entores v Miles Far East Corporation* (n 102).
[197] Weinrib, *The Idea of Private Law* (n 18) 138.
[198] *Dunlop v Selfridge* [1915] AC 847, 855.
[199] John N Adams and Roger Brownsword, *Understanding Contract Law* (5th edn, Sweet & Maxwell) 76.
[200] Robert Clark, *Contract Law in Ireland* (Eight edition, Round Hall Thomson Reuters 2016) para [2-06].

For consideration to be valid, it must be objectively or tangibly valuable. The value of the consideration needs only to be minimal, so a court will still enforce a contract where the value of the consideration is not equal to the subject matter of the contract. In this sense, consideration is evaluated juridically rather than economically.[201] On this point, Blackburn J. stated in *Bolton v Madden* that it is for the parties to decide whether or not the consideration is adequate.[202] Thus, in *Thomas v Thomas*, the Court held that the payment of £1 per annum by a widow to occupy a house was sufficient.[203] This judgment indicates that the threshold for consideration is quite low, therefore cryptocurrencies may constitute consideration even if a judge holds a negative view of them.

3.5 Intention to create legal relations

For an agreement to be legally binding, the parties must have intended to create legal relations. Technologists argue that smart contracts do not involve an intention to create legal relations, but that they are used simply for the management of digital assets. However, courts will use an objective test in deciding whether an intention to create legal relations exists within a particular arrangement. On this matter, Park J in the English High Court in *Hadley v Kemp* stated that the intention to create legal relations existed if a reasonable offeree interpreted the offer as including the intention.[204]

The judgment of Lord Clarke in the UK Supreme Court case of *RTS Flexible Systems Ltd v Molkerei Alois Muller GmbH* is instructive of what may constitute intent.[205] Importantly, he stated that it is irrelevant whether the parties subjectively did not intend to establish legal

[201] Mindy Chen-Wishart, 'In Defence of Consideration' (2013) 13 Oxford University Commonwealth Law Journal 209, 233.
[202] *Bolton v Madden* (1873) LR 9 QB 55.
[203] *Thomas v Thomas* (1842) 2 QB 851.
[204] *Hadley v Kemp* [1999] EMLR 589, 623.
[205] *RTS Flexible Systems Ltd v Molkerei Alois Muller GmbH* [2010] 1 WLR 753.

relations. Instead, he stated that the words or conduct of the parties must be assessed to determine whether they objectively result in the creation of legally binding relations.[206] Thus, where the parties have set out incomplete terms during pre-agreement negotiations, an objective assessment of their words or other conduct may indicate that they lacked the requisite intent to create legal relations.[207]

Traditionally, courts have held that agreements between family members were not intended to create legal relations.[208] However, commercial agreements are prima facie intended to create legal relations unless parties explicitly state otherwise. In this regard, Barrington J in *O'Rourke v Talbot (Ireland)* stated that there is a heavy onus on parties who assert that the agreement was not intended to be legally binding.[209] Only in limited circumstances might parties override common law principles of contract formation by declaring they do not intend to be legally bound by an agreement.[210] In *Hadley,* Park J. acknowledged that commercial arrangements usually involve an intention to be bound, but stated that courts may depart from this general rule.[211] He stated that there was no intention to create legal relations in the arrangement as the band was not set up only to make money, but also out of a passion for creating music.[212]

3.6 Legal validity of smart contracts

Before the substantive questions as to what happens when a smart contract is vitiated is answered, it is first necessary to determine whether a smart contract amounts to an agreement

[206] *RTS Flexible Systems Ltd v Molkerei Alois Muller GmbH* [2010] 1 WLR 753, 771.
[207] ibid.
[208] This position was established in *Balfour v Balfour* [1919] 2 KB 571, in which an agreement between a husband and wife was held as not legally binding. The presumption that legal relations do not arise also extends to other family members including an agreement between a mother and daughter. See *Jones v Padvatton* [1969] 2 All ER 616.
[209] *O'Rourke v Talbot (Ireland) Ltd* [1984] ILRM 587, 593.
[210] Raymond J Friel, *The Law of Contract* (Round Hall Press 1995) 79.
[211] *Hadley v Kemp* [1999] EMLR 589, 624.
[212] ibid.

that can be enforced in contract law. This section applies the law set out in the above section to determine whether contract law can recognise smart contracts as legal contracts.

3.6.1 Parameters affecting the mapping of smart contracts to corrective justice

Smart contracts do not substitute contract law, however they do contain certain characteristics which affect the how they can be mapped onto the concepts of traditional contract law. These characteristics will be discussed recurringly throughout the thesis as they factor into our analysis of the various contract law doctrines.

1. Identification and connection of parties

Given the bipolarity of the private law relationship, it is essential that there is a plaintiff and a correlative defendant to a smart contract dispute.[213] Depending on the extent of a smart contract's 'autonomy', the connection between two parties may be severed because the actions of the software may not be attributable to a particular plaintiff and defendant.[214] A smart contract is autonomous in the sense that performs its terms on its own without human involvement once it has been deployed on the blockchain.[215] Yet, regardless of their autonomy, all software is created and controlled by its human operator. The degree to which the human is removed from the transaction may make it more difficult to assert that they form part of a juridical relationship. If the smart contract is formed by way of an algorithm, the reciprocal connection between the parties may not be present.

Moreover, when parties use the blockchain to transact, their identity may become obscured. Smart contracting parties may be identifiable to one another only by their respective blockchain

[213] Weinrib, *The Idea of Private Law* (n 18) 28 (on the juridical relationship as it exists in private law).
[214] Pinchas Huberman, 'Tort Law, Corrective Justice and the Problem of Autonomous-Machine-Caused Harm' (2021) 34 Canadian Journal of Law & Jurisprudence 105, 116 (discussing the difficulty in connecting conduct by autonomous systems with a human party in tort law).
[215] Alexander Savelyev, 'Contract Law 2.0: "Smart" Contracts as the Beginning of the End of Classic Contract Law' (2017) 26 Information & Communications Technology Law 116, 127.

wallet number which consists of a string of alphanumeric characters.[216] The pseudonymity provided by the blockchain makes it difficult to identify one or both parties to the transaction. If the parties cannot be identified, the context in which the contract was entered into may not be understood because the necessary facts cannot be ascertained.[217]

Using smart contracts therefore differs from transacting in Web 2.0 where transactions are typically facilitated by intermediary marketplaces such as Amazon or Etsy which are obligated to obtain information of the parties under Know Your Customer requirements. Although the anonymity of smart contracts is considered by some commentators as one of the main benefits of transacting using the blockchain, ascertaining the meaning of the smart contract becomes challenging if the only item available to analyse is the smart contract's code.[218]

2. Expression of the smart contract's terms

The smart contract itself is a software programme written in computer code which facilitates the automatic execution of an agreement.[219] This may give rise to problems for contract law because the plaintiff's right and the defendant's duty are correlative.[220] The plaintiff must be able to identify how she has been wronged, which she can do by identifying how the defendant breached his duty, and in doing so, infringed her right.[221]

The correlative right and duty of the parties are readily identifiable if they have been expressed in a natural language. In such instances, the smart contract is being used to execute an agreement which the parties have already formed off-chain. The code of the smart contract may then be used to animate a significant chunk of their agreement, or a minute section of it.[222] The

[216] Mark Giancaspro, 'Is a "Smart Contract" Really a Smart Idea? Insights from a Legal Perspective' (2017) 33 Computer Law & Security Review 825, 828.
[217] Jasper Verstappen, 'A Smart Contract Taxonomy: An Instrument to Provide Insights in Legal Risks Created by Smart Contract Technology' (2024) 1 Compact 4.
[218] Sklaroff (n 181) 295.
[219] Filatova (n 19) 237.
[220] Weinrib, *Corrective Justice* (n 8) 20.
[221] ibid 20.
[222] Allen (n 47) 330–341.

content of the agreement may be communicated using a whitepaper, website, or email in a manner which the parties can easily comprehend, notwithstanding their knowledge of computer programming.

Otherwise, the smart contract may be presented entirely as a piece of code without a plain language agreement. The risk in this scenario is that parties become bound to the output of the code, notwithstanding defects in its performance. While a natural language agreement provides the courts with a framework to identify the mutual will of the parties, code in isolation operates mechanistically. Absent any alternative indication of the parties' intent, the parties, and the courts, may treat the 'code as the contract'.[223]

3. Smart contract immutability

Another factor which impacts how smart contracts map onto contract law, and how disputes should be remedied, is the immutability of smart contracts. While most forms of software can be upgraded or amended as necessary, the blockchain prohibits the *ex post* amendment of smart contracts once they have been deployed on it.[224] The blockchain is a decentralised ledger system wherein data is organised into a series of blocks that are sequentially interconnected. Cryptographic techniques are employed to guarantee the integrity of the blocks, preventing any modifications to them and thus rendering them tamperproof.[225] This means that smart contract transactions are difficult to unwind once they have been executed. As such, the party drafting the smart contract must ensure that its code provides exactly what both he and the promisee intend. Otherwise, the parties may have to find a way to reverse the effect of the smart contract's

[223] Daniel Drummer and Dirk Neumann, 'Is Code Law? Current Legal and Technical Adoption Issues and Remedies for Blockchain-Enabled Smart Contracts' (2020) 35 Journal of Information Technology 337, 341.
[224] Eliza Mik, 'The Resilience of Contract Law in Light of Technological Change' in Michael Furmston (ed), *The Future of the Law of Contract* (Informa Law 2020) 128.
[225] Agata Ferreira, 'Regulating Smart Contracts: Legal Revolution or Simply Evolution?' (2021) 45 Telecommunications Policy 102081, 3.

performance using offline measures.[226] Immutability therefore renders smart contracting as a significantly inflexible practice, and renders it difficult to place parties back into a pre-contractual position, per the requirements of corrective justice.[227]

4. Susceptibility to coding errors

One of the main problems of moving from natural language to computer code is the likelihood that errors will be coded by parties into the smart contract. Mik posits that 'statistically, *each* computer program contains such' errors.[228] In order to bring about the performance intended by the parties, it is necessary that there are minimal errors in the code. However, given that coding errors are so widespread, disputes will arise particularly for mistake and innocent misrepresentation where the performance of the smart contract does not reflect the promise made by the promisor. As any agreements which contain errors in their code cannot be amended, parties must carefully programme their smart contracts to avoid any defects in performances.[229] If the parties fail to ensure that the smart contract is free of any bugs, the likelihood of the infringement of the offeree's right increases, and may necessitate the rectification of their holdings to restore the equality in their transaction.

3.7 Formation of smart contracts

The first type of smart contract to be considered is the 'bilateral smart contract'. This category of smart contract is referred to as such because it is distinctly bilateral in its form. Its bilaterality

[226] Olaf Meyer, 'Stopping the Unstoppable - Termination and Unwinding of Smart Contracts' (29 October 2019) 14 <https://papers.ssrn.com/abstract=3537477> accessed 24 April 2024.
[227] Weinrib, *Corrective Justice* (n 8) 4.
[228] Mik, 'Smart Contracts' (n 2) 280.
[229] Larry A DiMatteo, Michel Cannarsa and Cristina Poncibò, 'Smart Contracts and Contract Law' in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019) 4.

is a result of its setup, wherein two parties commit to one another that they will undertake their own obligations under the contract.[230] The rights and the duties of the parties are set out in an off-chain, plain language agreement. The role of the smart contract is merely to give effect to the legal agreement by performing some, or all, of its terms automatically.[231] The following subsections assesses how bilateral smart contracts map onto contract law and the concepts of corrective justice.

3.7.1 Identifying an offer and acceptance in bilateral smart contracts

For an agreement to be legally binding, the first requirement is that there must be an offer that can be accepted by the offeree. Under common law, the offer must consist of a clear and unambiguous statement of the contract's terms. Whether a given smart contract maps onto contract law depends on its composition. For instance, a bilateral smart contract, the terms of which have been mutually agreed upon by the parties involved prior to the coding of those terms, will provide greater clarity than a decentralised anonymous smart contract that exists solely in coded form. The offer of the bilateral smart contract is found in an accompanying agreement formed off-chain before the smart contract was programmed.[232] The parties' correlative rights and duties are identified by referring to the conventional contract; the smart contract in this context merely performs the transaction.

An example of a bilateral smart contract transaction may involve the carriage and delivery of goods by sea.[233] The parameters of such a transaction is likely too complicated to set out in

[230] Essentially, bilateral smart contracts reflect the idea of traditional bilateral contracts which McKendrick states involves '... two parties to the contract [who] promise to each other that they will carry out their respective obligations under the contract (in other words, they exchange promises)' (emphasis added). See Ewan McKendrick, *Contract Law* (10th edn, Oxford University Press 2022) 44.
[231] Verstappen, 'A Smart Contract Taxonomy' (n 193) 4.
[232] Brownsword, 'Regulatory Fitness' (n 17) 21.
[233] An example set out by Brownsword. See ibid 18.

code-form only, for instance, the destination or the type of goods to be transported may be obscured if this information is buried within the software's code. As such, the parties may opt to form a conventional contract first, the offer of which would plainly state, for example, that the carrier will bring computer processing chips from Dublin to London for €10,000. Working in tandem with an oracle (a third-party data facilitator) the smart contract can issue payments when certain milestones have been reached (i.e. when the cargo has been loaded onto the ship, when the ship has docked, and when the cargo has arrived at its final destination). The content of the offer is found within the natural language document, of whose performance the smart contract merely exists to automate. In other words, the offer is a promise in its plainest form wherein the offeror states that he will undertake a specific course of conduct in the future.[234] The only difference here compared to a conventional contract is that his conduct is entrusted to computer code. Essentially, the rights and duties of the parties are understood according to the natural language document.

Reflecting the correlativity of contract law, the mirror image rule requires that the offeree's acceptance parallels the offer. As such, the acceptance must not deviate from the terms which were initially offered. Moreover, the acceptance of an offer in a bilateral contract must be communicated to the offeror. Therefore, an offeree may accept a bilateral *smart* contract by stating verbally that he assents to all the terms of the offer. Acceptance occurs similarly as it does to a conventional contract. Otherwise, a bilateral smart contract offeror may prescribe a certain mode of acceptance, and permit the offeree to accept the contract by way of conduct. This way, the parties can agree that acceptance occurs when the offeree interacts with the smart contract, by placing the stipulated amount of fiat, or cryptocurrency into it.[235]

---

[234] Arthur L Corbin, 'Offer and Acceptance and Some of the Resulting Legal Relations' (1916) 26 Yale Law Journal 169, 171.

[235] Mateja Durovic and André Janssen, 'Formation of Smart Contracts under Contract Law' in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019) 67.

3.7.2 DASC offers and acceptances

Bilateral smart contracts may be accepted either by express communication of assent or by conduct. However, where the transaction is entirely on-chain, an offer comes into existence once the offeror submits the smart contract to the blockchain.[236] The smart contract itself constitutes the offer, meaning that the offer is expressed entirely in computer code. In this context, the offer is not communicated in plain language by the offeror to the offeree. Filatova states that parties rarely use this type of smart contract as they tend to favour bilateral smart contracts.[237] However, DASCs are used throughout the blockchain community. The transaction of the CryptoPunk #2386 NFT demonstrates how smart contracts may exist on the blockchain without an accompanying natural language offer. The asset was purportedly worth $1.5 million; however, it was acquired for a significantly lower amount on the open market.[238] The offer was originally made via an NFT marketplace which had become defunct. When it became defunct, the front-end of the marketplace's website was rendered offline but the smart contract could still be accessed via blockchain interfaces like 'etherscan.io'. The smart contract existed independently of other written terms governing the transaction, and the code alone therefore governed the transaction.

The CryptoPunk smart contract was an anomaly because it once had a webpage explaining its content. However, many smart contracts are deployed on the blockchain on a daily basis and are accessible directly via a blockchain interface. The information available to an offeree through the interface consists of the contract's source code and raw, technical data. Durovic

[236] ibid.
[237] Filatova (n 19) 234.
[238] Nizan Geslevich Packin, 'The CryptoPunk Drama: Is "Code Is Law" Cracking Under Pressure?' (*Forbes*) <https://www.forbes.com/sites/nizangpackin/2024/09/16/the-cryptopunk-drama-is-code-is-law-cracking-under-pressure/> accessed 17 September 2024.

and Janssen argue that even where the smart contract is available only in code form, it may still constitute an offer once it is deployed on the blockchain so long as the code is sufficiently specific in setting out the contract's terms.[239] However, the opacity of computer code may sometimes render it difficult to ascertain a smart contract's terms. In particular, smart contracts that are both formed and executed by way of code, including DASCs and DAOs, evade contractual status because the purported offer lacks intelligibility. If the code is not comprehendible to its recipient, then it is not possible for him to be *ad idem* with the smart contract's offeror. Without the requisite meeting of minds of the parties, the offeror does not ascertain a duty to perform and the offeree does not acquire a right to his performance. To demand otherwise would conflict with the offeree's purposiveness.

The tension between computer code capable of acceptance and code that is not was borne out in *Quoine Pte Ltd v B2C2 Ltd*.[240] In that case, both parties used deterministic algorithms which resulted in the trading contract between them. Menon C.J. stated that neither B2C2 or the involved counterparties would have known that an offer or acceptance was made.[241] Moreover, he stated that they could not anticipate what the terms of the contract would ultimately be because they would also be determined by the algorithm. Notwithstanding these factors, the Majority found that a valid contract existed. They arrived at this conclusion by referring to the English High Court decision in *R (on the application of Software Solutions Partners Ltd) v Her Majesty's Commissioners for Customs and Excise)*.[242] There, an automated electronic form of contracting was also used whereby insurance brokers could generate insurance policy quotes by inputting data into the system. The programme automatically determined the customer's

[239] Durovic and Janssen (n 28) 67–68: ['However, as the 'offeror' posts his 'contract' on the blockchain in a binary computer code that specifies precisely the terms of the transaction, it will regularly be held to be exact enough to constitute an offer and not only an invitation to treat.'].
[240] *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA (I) 02.
[241] ibid 78.
[242] *R (on the application of Software Solutions Partners Ltd) v Her Majesty's Commissioners for Customs and Excise* [2007] EWHC 971.

risk and, by itself, determined if the risk was acceptable. Based on the outcome of its calculation, the programme would make an offer to the customer without deferring back to the insurance company. Once the customer accepted the quote, the contract between the insurer and the customer was automatically generated by the software. The Court in *Software Solutions Partners* found that the contract was binding by analogising the facts of that case to *Thornton v Shoe Lane Parking Ltd*, where Lord Denning M.R. found that the offer was made when a vending machine's owner placed it as ready to take payment, and acceptance was made by inserting money into the designated slot.[243]

The vending machine offer in *Thornton* may be analogised to a bilateral smart contract as the details regarding the transaction may be found on or around the machine. It is less certain that *Thornton* explains DASCs. This is because both the offeror and the offeree in that case are active participants in the transaction, and the use of a vending machine does not diminish the role of the offeror. Although in *Thornton*, the Court found that an exclusion clause was not incorporated into the contract because it was not brought to the plaintiff's attention, it was still possible to identify some of the contract's terms. Had the exclusion clause been identified to the plaintiff before the contract was formed, then the defendant may have succeeded in its argument. If the contract and its incorporated terms are in a plain language, then there is less noise to cut through to identify what is the contract. The parties may reasonably know (1) when a contract has been formed, and (2) the terms to which they have agreed.[244]

An algorithmic smart contract on the other hand obfuscates the role of one party, or the other. By upholding some coded agreements, the risk is that parties are not respected as autonomous agents. This is why the contract in *Quoine* would likely not be regarded as a contract according to the corrective justice standard. A contract is supposed to be 'a manifestation of equal freedom

[243] *Thornton v Shoe Lane Parking* [1971] 2 QB 163, 169.
[244] Had notice of the exclusion clause been properly placed, that is.

entered into by two self-determining agents'.[245] Yet, the parties in *Quoine* were not self-determining agents. They did not know that an offer and acceptance would be made, or what ultimately would be the terms of the contract if it materialised. Their self-determination was limited to the act of deciding to use algorithms to form agreements on their behalf. However, this act precedes the correlative process of making an offer and acceptance and falls outside the scope of the contract's formation. Therefore, it is not certain that a DASC is a contract at all.

The Court in *Quoine* would likely be dissatisfied with this argument. Although the parties did not know that they would enter into a contract or what its terms would be, the Court was, nonetheless, content that an algorithm forms a valid contract if the parties are willing to adhere to its output.[246] But, the outcome of the algorithm did not reflect the will of the parties. How could it if they did not know that a contract would be formed between them in the first place, or what its terms would be? It is on this point that this thesis differs from the status quo of the existing scholarship, and of the decision of the Court in Quoine. For instance, the submission of a smart contract to the blockchain alone has been regarded as the potential source of an offer and acceptance.[247] As such, this thesis submits that the purported 'offer and acceptance' in a DASC are insufficient to lead to the conclusion of a legal contract between the parties.

To make the point clear, under a corrective justice account of contract law, one party's conduct must be compatible with the other party's freedom.[248] Quoine did not freely enter into the transactions at the centre of the dispute in that case. Instead, those interactions were brought about by the contract's code, the effect of which the parties could not have anticipated. Using

[245] Botterell (n 15) 108.
[246] *Quoine Pte Ltd v B2C2 Ltd* (n 216) [97].
[247] Filatova (n 19) 225.
[248] Weinrib, *Reciprocal Freedom* (n 33) 42.

code in this way disrupts the 'relationship of will to will' as the parties are reliant on the code to determine what is best for them when they do not know what that outcome might be.[249]

3.7.3 Advertisements on crypto asset marketplaces

A crypto asset transaction may begin when a party identifies an NFT on an online marketplace (such as OpenSea.io) which they would like to buy. In practice, these marketplaces operate similarly to websites such as Amazon or eBay, on which NFT creators can submit their work which can be bought by interested parties. The only difference between these two types of websites is that 'Web 2.0' sites such as Amazon facilitates the sale of mostly physical and non-crypto related products. 'Web 3.0' websites, like OpenSea.io and Nifty Gateway, are instead focused on the exchange of crypto assets including cryptocurrencies and NFTs. On these sites, a buyer can browse through a myriad of categories until they find an item that they desire. The question of whether such an advertisement constitutes an offer or an invitation to treat merits further analysis.

Where an advertisement for a crypto asset on an online marketplace is sufficiently specific, *Lefkowitz v Great Minneapolis Surplus Store* suggests that such an advertisement amounts to an offer.[250] Essentially, *Lefkowitz* revolved around the promise of a performance in return for a performance. The sale of an NFT through an online marketplace can be characterised as such, in that, the seller offers to transfer the NFT to the buyer when he has sent a specified amount of cryptocurrency to her. The details provided may also inform potential buyers about what level of ownership they will acquire over the underlying asset once they purchase the NFT.[251]

---

[249] ibid.
[250] *Lefkowitz v Great Minneapolis Surplus Store* (1957) 86 NW 2d 689.
[251] Michael Dowling, 'Fertile LAND: Pricing Non-Fungible Tokens' (2022) 44 Finance Research Letters. A common misconception of NFTs is that the asset (usually a digital image, audio file, virtual property) itself is the NFT. However, the NFT actually consists of the right to the underlying asset which is then recorded on the blockchain.

Although the *Lefkowitz* decision long predates the internet, it is indicative that the advertisement of an NFT on an online marketplace is an offer. This is because a definite sale price is provided which is not open to negotiation by the parties.

Moreover, online transactions no longer warrant the protection traditionally provided by the invitation to treat rule. Technological measures can be coded into a website's infrastructure which prevent buyers from ordering goods which are low in stock.[252] Smart contracts should, in theory, be proficient in restricting acceptances in such scenarios. However, even if such measures are not deployed, or fail, the application of the rule in *Grainger & Sons* may turn on the nature of the asset being sold. For instance, an NFT by its nature is non-fungible and there may be a limited number of similar NFTs in existence. In contrast, a significant amount of a specific cryptocurrency may be held by one individual. Therefore, a party may hold only a limited amount of a specific type of NFT and therefore a statement may constitute an invitation to treat, while a statement concerning a class of cryptocurrency may be an offer. Unless there is an offer which is matched by a correlative acceptance, the smart contract is not an enforceable one because an invitation to treat does not itself render a voluntary assumed correlative adjustment to the parties' positions if 'accepted'.[253] The reason being that it is not possible to accept an invitation to treat because the inviter's holdings will not change as a consequence of outlining his willingness to negotiate.

3.7.4 The irrevocable agreement

Traditionally, an offeror may revoke her offer before it has been accepted by the offeree, therefore it is necessary to determine at what point a smart contract is deemed accepted. The

[252] Mik, 'Certainty at Last?' (n 187) 171.
[253] Weinrib, *Idea* (n 14) 137.

reason is that the acts of offer and acceptance are separated in time, meaning that there is still an opportunity for the party to retract his willingness to change his moral position.[254]

To determine when acceptance has occurred, the courts apply the 'postal rule' where the offeree has used a form of non-instantaneous communication (such as a letter sent via the postal service). Under this rule, acceptance occurs when the offeree deposits the letter of acceptance into the post box.[255] If the blockchain is analogous to a post office which merely passes the notice of acceptance of a smart contract to the offeror, then acceptance may occur the moment the offeree interacts with the smart contract. However, a smart contract is not accurately characterised as a non-instantaneous form of communication because its acceptance occurs rapidly once it has been executed by the offeree.

To account for instantaneous modes of acceptance, the courts established the 'receipt rule' whereby acceptance occurs once the offeror receives the offeree's acceptance.[256] Such instantaneous communications may include verbal acceptance either in-person or over the telephone, as well as fax machines.[257] It is likely that the acceptance of a DASC would fall under the receipt rule because its acceptance is communicated instantaneously to the offeror. Moreover, the DASC is automatically performed once the offeree interacts with it, meaning that the offeror does not have to manually perform its terms. Once the offeree submits consideration to the smart contract, the transaction is instantly finalised and recorded on the blockchain.[258] In other words, the blockchain does not intermediate the formation process in

---

[254] ibid.
[255] *Household Fire and Carriage Accident Insurance Company (Ltd) v Grant* (1878) LR 4 Ex D 216, 221: ['But if the post office be such common agent, then it seems to me to follow that, as soon as the letter of acceptance is delivered to the post office, the contract is made as complete and final and absolutely binding as if the acceptor had put his letter into the hands of a messenger sent by the offerer himself as his agent to deliver the offer and receive the acceptance'].
[256] *Mondial Shipping and Chartering BV v Astarte Shipping Ltd* [1995] CLC 1011.
[257] Jan M Smits, *Contract Law: A Comparative Introduction* (3rd edn, Elgar Publishing 2021) 60.
[258] Simon Gleeson, 'Legal Considerations Around Smart Contracts: Contracts Between Computer Programs' (Social Science Research Network, 16 September 2021) 2 <https://papers.ssrn.com/abstract=3925127> accessed 13 May 2025.

the same way as the regular postal service. Given that there is typically no delay in the receipt of a smart contract's acceptance, there is no need for the postal rule to apply because the offeree will know immediately whether his acceptance has been successful.[259]

However, the offeror may encounter difficulties in revoking a DASC once it has been deployed on the blockchain. This is due to the DASC's immutability which prevents the parties from modifying its code post-submission to the blockchain.[260] In practice, this means that an offeror cannot revoke their offer from the moment the smart contract is uploaded. The case law on revocation is indicative of the reasons why an offeror might want to revoke his offer. For example, in *Dickinson v Dodds*, the defendant offered to sell his house to the plaintiff but subsequently revoked his offer because it was 'too late' as he had already sold the property in the interim.[261] A similar scenario may occur in a crypto asset transaction where one party might offer for sale an NFT, and thus code a smart contract to facilitate the trade. She might then change her mind and decide to sell it to a third party. She is entitled to withdraw her offer so long as the offeree has not yet accepted it. However, she may not be able to revoke her offer due to the immutability of smart contracts. Although, if she had anticipated that she might withdraw her offer, she could code into the smart contract a 'self-destruct' command.

During the formative period of the Ethereum blockchain, its creators enabled the implementation of a self-destruct function in smart contracts which permitted smart contract developers to terminate a smart contract. Although the self-destruct function is often used for security reasons to delete a contract which contains vulnerabilities, it may also be used to terminate a smart contract which the offeror no longer needs.[262] The ability to code this function

[259] Pang Wenn Ler, 'You've Got Mail: Examining the Postal Rule in the Technological Age' (2019) Singapore Comparative Law Review 35, 37.
[260] Jiachi Chen and others, 'Why Do Smart Contracts Self-Destruct? Investigating the Selfdestruct Function on Ethereum' (2021) 31 ACM Transactions on Software Engineering and Methodology 30:1, 2.
[261] *Dickinson v Dodds* (1876) 2 Ch D 463 at 464.
[262] For a discussion on possible motivations to include a self-destruct function in a smart contract, *see* Chen and others (n 234) 9–10.

into a smart contract reduces the effect of smart contract immutability on contract law regarding revocation as it enables an offeror to terminate her offer prior to its acceptance.

However, the offeror must communicate her revocation of the offer to the offeree.[263] In such a scenario, the identifiability of the offeree is important because it may be difficult for the offeror to inform the offeree if she does not know who he is or how to contact him. If it is a bilateral smart contract between both parties, they may know each other and have an off-chain means of communication with one another. However, if a unilateral, decentralised autonomous smart contract is used by the parties, then communication of revocation may be more difficult. For example, if an offeror places for sale an NFT on crypto asset marketplace which is open to the internet at large, revocation of the smart contract may be practically difficult. In such circumstances where the offeree is unidentifiable and direct communication is impossible, the offeror would have to notify potential offerees of the revocation of the smart contract through the same means as she advertised the sale.[264] Therefore, she would have to submit a post on the marketplace notifying that the NFT is no longer for sale. There is however no guarantee that this notice will reach its intended audience, and the underlying smart contract may still be 'accepted' notwithstanding the offerors intention to revoke the smart contract.

3.7.5 DAO Offers and acceptances

3.7.5.1 Defining DAOs

Before analysing DAO smart contracts now and throughout the rest of the thesis, this section will first provide a detailed explanation as to what a DAO is. By introducing the reader to the

[263] *Dickinson v Dodds* (1876) 2 Ch D 463 at 475.
[264] *Shuey v United States* (1875) 92 US 73.

characteristics specific to DAO smart contracts, it may make more sense why DAOs may constitute a hard fit with corrective justice, and therefore contract law.

DAOs are blockchain-based organisations comprised of a network of smart contracts, which operate through rules that are encoded in software. Given that traditional companies are comprised of a nexus of contracts, it may be beneficial to encode those agreements in the form of self-executing digital contracts.[265] It is through these coded rules that a DAO manages its users and its resources with minimal human intervention.[266] Stock ownership, corporate governance rules and the handling of payroll can be assigned to computer code through smart contracts rather than relying on human employees to carry out these routine tasks.[267] Another idea that underpins the DAO is that it should be developed and run by communities instead of relying on traditional hierarchies that are governed by centralised leaderships.[268]

To function, a DAO needs cryptocurrency; usually in the form of Ether because DAOs are typically hosted on the Ethereum blockchain.[269] To obtain the requisite Ether, the DAO can sell its own native crypto-token.[270] This way, a DAO can fund its activities (commercial or otherwise) similarly to how traditional companies sell shares to raise capital. In return for buying the DAO's native token, investors receive certain rights relating to the DAO.[271] The two core components of DAOs are their decentralisation and their purported autonomy.

[265] Werbach and Cornell (n 12) 337.
[266] 'Decentralised Autonomous Organisations Scoping Paper' (*Law Commission*) 8 <https://lawcom.gov.uk/document/decentralised-autonomous-organisations-scoping-paper/> accessed 15 August 2024.
[267] Werbach and Cornell (n 12) 337.
[268] 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 10.
[269] Alternative blockchains are also available now which facilitate the creation of DAOs (e.g. Solana). For the sake of simplicity, the Ethereum blockchain is referred to here.
[270] Carla L Reyes, 'If Rockefeller Were a Coder' (2019) 87 George Washington Law Review 373, 387.
[271] ibid.

3.7.5.2 Decentralisation

The ideal-type DAO is purely decentralised, however this is a difficult threshold to reach because usually some level of control is required by the DAO's ownership during its early developmental stages.[272] Ultimately however, the goal is to advance toward a model of community governance wherein the DAO's participants are entrusted with important decisions pertaining to the DAO. One prominent example of a DAO operated in this manner is MakerDAO, which exists to generate the 'stablecoin' Dai.[273] Users who hold MakerDAO's native token, MKR, have a right to vote on amendments to the DAO's protocol and the management of its treasury.[274] They have an economic incentive 'to act in the best interest of the platform' because the value of the DAO's token could increase based on the DAO's good performance.[275] However, MakerDAO was governed during its formative years by the 'Maker Foundation' which was responsible for managing the protocol of the DAO until such a point that the token holders were prepared to deal with its management. The Foundation was gradually phased out, thus leaving MKR token holders in charge of its software development, upgrades and maintenance, and promoting it to others to achieve some level of commercial success.[276]

Blockchain technology makes this level of decentralisation possible by enabling parties to transact without having to trust one another. Specifically, the integrity of transactions is ensured by the blockchain's use of public-key cryptographic protocols.[277] This way, the technology

---

[272] 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 39–40.
[273] 'MakerDAO' <https://makerdao.com/en> accessed 11 December 2024; A stablecoin is a cryptocurrency to established assets like fiat currencies, like the USD dollar, or commodities such as silver. See Chainalysis Team, 'Stablecoins 101: Behind Crypto's Most Popular Asset' (*Chainalysis*, 11 December 2024) <https://www.chainalysis.com/blog/stablecoins-most-popular-asset/> accessed 3 June 2025.
[274] Michael Anderson Schillig, 'Decentralized Autonomous Organizations (DAOs) under English Law' (2023) 0 Law and Financial Markets Review 1, 4.
[275] ibid.
[276] Brady Dale, 'MakerDAO Moves to Full Decentralization; Maker Foundation to Close in "Months"' (*CoinDesk*) <https://www.coindesk.com/tech/2021/07/20/makerdao-moves-to-full-decentralization-maker-foundation-to-close-in-months> accessed 11 December 2024.
[277] Jasper Verstappen, 'Regulating Unfair Commercial Practices in a Smart Contract Context' (2024) 15 European Journal of Law and Technology 4.

authenticates the transacting parties and ensures that parties cannot repudiate once a smart contract has been executed on the DAO's network.

Another benefit of decentralisation is that transactions are censorship resistant. As such, it is difficult for any institution or individual to unilaterally reverse or block transactions once they have been executed via smart contract.[278] The reversal of transactions is possible, but rendered difficult by the blockchain's protocols. This is demonstrated by the cyber-attack conducted against *TheDAO*. *TheDAO* was one of the first high-profile organisations to combine smart contracts in the form of a network to create a DAO. It functioned as a decentralised virtual capital fund in which its participants voted to determine which projects should receive funding. It successfully raised $150 million worth of Ether cryptocurrency during a crowd sale but suffered a major setback when attackers identified and exploited vulnerabilities contained in the code of one of its smart contracts.[279] Through the attack, the attackers were able to siphon off approximately $60 million of the Ether that had been accumulated by *TheDAO* and its participants. Due to the immutability and censorship-resistant nature of DAOs, its founders were unable to unilaterally reverse the transactions which the attackers had executed using the loopholes contained in the smart contract's code. However, its participants were entitled to vote on a technological rather than legal solution; to perform a 'hard fork'. The hard fork involved implementing software updates relating to the Ethereum blockchain that resulted in the creation of a new version of the Ethereum blockchain but did reverse some of the illegitimate transactions, returning funds to harmed investors. The economic incentive to support *TheDAO* thus succeeded over the notion that the blockchain should be fundamentally unchangeable, and its transactions irreversible.[280]

---

[278] Claudia Biancotti, 'What's Next for Crypto?' (Social Science Research Network, 21 September 2022) 32 <https://papers.ssrn.com/abstract=4462817> accessed 12 December 2024.
[279] Werbach and Cornell (n 12) 350–351.
[280] Wouter Dammers, 'How to Govern King Code' in Liisa Albertha Wilhelmina Janssens (ed), *The Art of Ethics in the Information Society: Mind You* (Amsterdam University Press 2016) 37.

3.7.5.3 Autonomy

In order to be decentralised, DAO's require a degree of autonomy. Autonomy in the context of DAOs has two meanings. The first is autonomy in the sense that external institutions and entities should have limited control over a DAO. When a DAO maximises its level of autonomy in this way, it seeks to escape the reach of regulators, the state, the courts, banks, and internet service providers.[281] Instead, the DAO will try emphasising its own governance rules and to exclude interference by these institutions. The desire to escape this interference derives from the broader objective of blockchain technology to move away from 'inefficient and corruptible institutions' and the law and lawyers in favour of private ordering.[282] Consequently, the participants of many DAOs assent to being ruled by the software code which constitutes the DAO.[283]

The second meaning of autonomy in the DAO context refers to the automation of its processes. This automation is facilitated using smart contracts that use self-executing code to automatically implement rules which have been predefined by the DAO's participants and its developers. This type of autonomy closely relates to the overall objective of DAOs, namely that they ultimately strive to 'take on a life of [their] own' and use code to co-ordinate the actions of multiple participants to achieve a common purpose.[284] In this regard, the founders of the organisation ultimately have a limited command over the DAO, and algorithms instead orchestrate the actions of the firm. All the DAO needs to function then is a body of code which serves the functions its developers initially sought to achieve, and funds which are provided by

[281] 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 18.
[282] Sklaroff (n 181) 268; Ferreira (n 201) 5.
[283] Aaron Wright, 'The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges' (2021) 4 Stanford Journal of Blockchain Law & Policy 152, 153.
[284] Alexandra Sims, 'DAOs (Decentralised Autonomous Organisations) v DINOs (DAO in Name Only or Decentralised in Name Only)' (5 February 2024) 3 <https://papers.ssrn.com/abstract=4716559> accessed 7 May 2024.

its membership when they assent to becoming a participant.[285] Once these elements are present, a DAO can act in any way for which the code was designed. This includes manners which are contrary to the will of the DAO's participants, as will be discussed in the following sections of this chapter.[286]

The UK Law Commission has identified a category of DAO which strictly pertains to the ideal of autonomy which it calls 'pure DAOs'. Pure, or algorithmic, DAOs are an 'extreme' version of DAO where all its processes are managed by computer code and algorithms.[287] These are the closest version to DAOs as they were originally conceptualised.[288] They are of particular concern because they are governed predominantly by their code and therefore the code will primarily govern the 'contractual relations' that arise out of the DAO.[289]

In pure DAOs, multiple parties are connected with each other to create projects with a common purpose. The activities of such a DAO are conducted algorithmically and in accordance with its computer code.[290] Within the code, the developers can set out the DAO's purpose, the roles and responsibilities of its participants, the incentive structure for participating, and instructions for treasury management.[291] Once these elements have been set out by the original developers, the DAO can theoretically operate with minimal human intervention going forward. The parties need not know each other to participate in the organisation. Hence, a single DAO may have

[285] André Guskow Cardoso, 'Decentralized Autonomous Organizations - DAOs: The Convergence of Technology, Law, Governance, and Behavioral Economics' [2023] MIT Computational Law Report 5 <https://law.mit.edu/pub/decentralizedautonomousorganizations/release/1>.
[286] ibid.
[287] The UK Law Commission uses the term 'Pure DAO' to describe DAOs predominantly run using code. Borgogno and Martino call these 'Algorithmic DAOs'. Both terms are interchangeable, but for the purpose of this article, I will adopt the Law Commission's term. See 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 39; Oscar Borgogno and Edoardo Martino, 'Decentralised Autonomous Organisations: Targeting the Potential beyond the Hype' (2024) 0 Law, Innovation and Technology 1, 6.
[288] 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 39.
[289] Contrast with 'digital legal entities', a type of DAO which forms only part of an existing business. Unlike pure DAOs, digital legal entities are incorporated like traditional companies and operate using traditional corporate governance measures. See ibid 98.
[290] Blaise Carron and Valentin Botteron, 'How Smart Can a Contract Be?' in Daniel Kraus, Thierry Obrist and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Edward Elgar Publishing 2019) 110.
[291] 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 21.

participants from multiple jurisdictions, all contributing to its development, as well as to attain a particular objective.

3.7.6 The Legal Classification of DAOs

DAOs are a novel creation that bring together numerous participants and co-ordinates them predominantly using computer code. Participants become involved in a DAO by executing a smart contract in order to receive the DAO's native crypto-token. Notwithstanding their novelty and technological basis, the law provides a framework through which the courts can assess the relationship between participants. On one end of the spectrum, there is the relatively unproblematic 'digital legal entity' DAO type defined by the UK Law Commission as an incorporated association which follows the formal procedures associated with traditional companies but that use blockchain technology to govern their organisation.[292] They may therefore be registered as limited liability companies and thus have separate legal personality, and can consequently enter into contracts as a company.

Additionally, there is the 'hybrid arrangement' wherein a company is formally registered but uses smart contracts and the blockchain to automate only certain parts of their business.[293] The portion of the company which is governed using code will be decentralised and autonomous relative to the rest of the organisation, which operates under a centralised hierarchy. Thus, important decisions relating to the company's governance are still made by a board of directors as opposed to all of its token-holders broadly.[294]

Relative to both the digital legal entity and the hybrid arrangement, the pure DAO does not involve the formal registration of the organisation, and the organisation is strictly embodied in

[292] ibid 40.
[293] ibid 40.
[294] ibid.

the computer code. It therefore does not have separate legal personality, and consequently cannot enter contracts. Instead, the pure DAO may constitute an unincorporated association.

The judgment by Orrick J. in *Commodity Futures Trading Commission v Ooki DAO* is instructive in determining the legal nature of DAOs, and of their underlying smart contracts.[295] The CFTC in that case successfully argued that Ooki DAO was operating an illegal trading platform and that it was illegally selling futures commissions. Specifically, the CFTC was acting under its mandate to enforce regulations under the Commodity Exchange Act. The CFTC could only take action against an entity which constitutes a 'person' subject to the Act, and the definition for 'person' under the Act also includes 'associations'. Thus, the dispute centred on whether the CFTC could persuade the Court that Ooki was an association.

The applicable law in that case, California State law, states that an unincorporated association is 'an unincorporated group of two or more persons joined by mutual consent for common lawful purpose, whether organized for profit or not'.[296] Orrick J. found that Ooki DAO satisfied this definition because, on the first criterion, it demonstrated that there were two or more participants involved in the organisation. In arriving at this finding, he rejected the argument made by the amici who argued on behalf of Ooki DAO that DAO's were not a collective of people, but a 'technological tool'.[297]

On the second criterion of mutual consent, the amici argued that 'different persons casting different votes at different times does not constitute mutual consent'.[298] However, the Judge held that this was based on a misinterpretation of the requirement. Instead, the focus of the law is on whether both parties consented to the participant joining the organisation. By executing

[295] *Commodity Futures Trading Commission v Ooki DAO* [2022] Northern District of California Case No. 3:22-cv-05416-WHO.
[296] Cal. Corp. Code § 18035(a), quoted at section Discussion (I)(C) in ibid.
[297] ibid.
[298] ibid.

the smart contract to purchase Ooki DAO's token, the participant was providing his consent to joining the organisation.

In relation to the third criterion, the Court held that Ooki DAO had a common lawful purpose to render it an unincorporated association. It found that the common purpose that unified the organisation's participants was the governance of the DAO by using and distributing the funds contained within its treasury.[299] It was immaterial that the participants did not always vote on proposals in similar ways, or abstained from voting altogether. Once the participant is part of the organisation, whether he chooses to vote or not is a voluntary choice and he is free to sell the token as he deems appropriate.[300]

Additionally, the Court in *Van Loon v Department of Treasury* for similar reasons found that the DAO involved in that dispute, Tornado Cash, constituted an association.[301] Similarly to the amici in *CFTC v Ooki*, the plaintiffs argued that Tornado Cash was not an association but an 'open-source software project comprised of a subset of smart contracts' hosted on the Ethereum blockchain.[302] However, Pitman J. rejected this argument because Tornado Cash was comprised of a group of individuals in the form of its founders, developers, and contributors rather than an abstract software project.[303] Moreover, he found that they had a common purpose in governing, promoting and developing Tornado Cash.

Given that many pure DAOs operate on a similar basis to both Ooki and Tornado Cash, the judgments in *Ooki DAO* and *Van Loon* will be instructive as to how the courts in common law jurisdictions should classify DAOs that do not conform to traditional corporate form. Therefore, instead of constituting a limited liability company, many DAOs will take the form

[299] ibid.
[300] ibid.
[301] *Van Loon v Department of Treasury* [2023] Western District of Texas 1:23-CV-312-RP.
[302] At section Order (I) in ibid.
[303] At section (III)(A)(1) in ibid.

of unincorporated associations run for profit. It would be inaccurate to hold that DAOs are merely technological tools or pieces of software devoid of any legal characteristics. As such, the contractual relations in a DAO will likely take the form of multilateral contracts between the various participants of the organisation.

3.7.7 The Nature of DAO Contracts: Multilateral Smart Contracts

If a DAO is an unincorporated association, then it may involve the creation of multilateral smart contracts rather than straightforward, bilateral smart contracts. The difference between these two types of contract is not entirely based on the amount of parties to the contract, but instead on the nature of the parties' rights and duties created under the contract.[304] In a multilateral contract, the parties do not perform in return for the performance of others, and instead it involves the pooling of resources together.[305] These resources are then used to advance a collective purpose.

This definition of multilateral contract applies to DAO-based smart contracts because they pool resources together to achieve the common purpose of the particular DAO. The resources may take the form of funds (often cryptocurrency), computer processing power, or expertise. For example, MakerDAO, discussed earlier in this chapter, involves the pooling together of funds which can be used as collateral and to maintain the DAI stablecoin governed by MakerDAO. Another example is ConstitutionDAO where participants collectively submitted funds to raise money to bid on a rare copy of the U.S. Constitution at auction.[306] In Golem Network DAO, participants contribute their computer processing power so that others can use that power for

[304] Irina Sakharova, 'The Power to Contract and the Offer-and-Acceptance Analysis of Contract Formation' (2024) 37 Canadian Journal of Law & Jurisprudence 261, 273.
[305] ibid.
[306] Karen Matthews, 'Rare First Printing of US Constitution Sells for Record $43M' *AP News* (19 November 2021) <https://apnews.com/article/cryptocurrency-technology-lifestyle-business-arts-and-entertainment-b0ab721a52cf20f2dc1a923f2dae3347> accessed 13 December 2024.

processing-power intensive tasks like machine learning, complex calculations, and CGI rendering.[307]

Peel argues that it is 'impossible or highly artificial' to assess multilateral contracts based on the traditional offer-and-acceptance model of contract formation, and that these are the exception to the requirement of offer and acceptance.[308] The purpose of this section is to assess this claim with regard to DAOs. Nonetheless, it would be advantageous for participants who subsequently seek to enforce their rights under a DAO contract if the courts overlook the formalities of formation. For example, Richards L.J. in *Premier Paper Group Ltd v Buchanan McPherson Ltd* found that the courts may downplay the significance of 'the precise mechanics of offer and acceptance' where it is otherwise clear that the parties had formed an agreement.[309] Hence, the courts will permit an offeror to infer an agreement from the offeree's performance of the contract's terms.[310]

3.7.8 Offer and Acceptance of the Coded Contracts of DAOs

The first step is to assess the formation of DAO based contracts to determine whether there is a binding and enforceable contract notwithstanding the lack of a natural language agreement. The functions of these contracts vary, but typically involve the governance of the DAO, managing voting on proposals, paying contributors and developers, and administering the sale of tokens. By clarifying whether a binding contract exists, token holders can be assured as to whether they have a right to vote or a share in the profits of the DAO, while users of a DAO's underlying product or service require clarity as to their rights should the product or service not

[307] 'About' (*Golem Network*) <https://golem.network/about> accessed 13 December 2024.
[308] Edwin Peel, *Treitel's The Law of Contract* (14th edn, Sweet & Maxwell 2015) 52.
[309] *Premier Paper Group Ltd v Buchanan McPherson Ltd* [2018] EWCA Civ 15 [29].
[310] *Brodgen v Metropolitan Railway Company* (1877) 2 AC 666.

be delivered as expected.[311] Other contributors such as validators who are responsible for verifying the transactions that take place between the DAO and its users may wish to determine whether they have an enforceable right against the DAO's ownership should they not be remunerated for their service.[312] DAO smart contracts have evaded academic analysis from a strictly contractual point of view, and the scholarship often focuses on the corporate form of the DAO, and other potential regulatory responses to DAOs.[313] This thesis provides an early exposition of DAO smart contracts as a distinct form of smart contracting, and ultimately finds that they constitute multilateral contracts, and consequently, may not establish the bilateral nexus between a certain plaintiff and defendant.

To determine whether parties have arrived at an agreement, the courts are not concerned with their subjective state of mind, and will instead focus on what was actually communicated between them through their words or conduct.[314] This requirement aligns with Weinrib's argument that the 'purely mental imaginings and reservations' of the parties 'have no status in this world of interaction'.[315] Therefore, it will be easier to identify the objective intentions of the parties where the parties have agreed to contractual terms before the smart contract is created.[316] However, where this communication is absent, the courts may find it difficult to ascertain any agreement at all.[317]

One type of 'agreement' identifiable within a DAO's framework is that between the DAO and users who validate transactions. Validators play a crucial role in the operation of the DAO (and

[311] 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 70.
[312] ibid 71.
[313] For example, see Aaron Wright, 'The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges' (2021) 4 Stanford Journal of Blockchain Law & Policy; Michael Anderson Schillig, 'Decentralized Autonomous Organizations (DAOs) under English Law' (2023) 0 Law and Financial Markets Review 1; Alexandra Sims, 'Blockchain and Decentralised Autonomous Organisations (DAOs): The Evolution of Companies?' (1 November 2019) <https://papers.ssrn.com/abstract=3524674> accessed 12 July 2024.
[314] *RTS Flexible Systems Ltd v Molkerei Alois Muller GmbH & Co (UK Production)* [2010] 1 WLR 753 [45].
[315] Weinrib, *Idea* (n 14) 104.
[316] Durovic and Janssen (n 28) 67.
[317] Although some courts have found that agreement may be found in contracts made in the form of computer code. For example, see *B2C2 Ltd v Quoine Pte Ltd* (n 127); and see *Quoine Pte Ltd v B2C2 Ltd* (n 216).

for blockchains broadly) as they ensure that transactions are processed without reliance on a centralised authority. In so doing, they ensure that the parties have sufficient funds to fulfil the transaction, and that the transaction follows the rules of the network.[318] Additionally, they ensure the integrity of the network by scanning the blockchain for malicious activity like double-spending.[319] In return for their work, they may expect to be remunerated with transaction fees in the form of the cryptocurrency that is native to the blockchain upon which the DAO is hosted (usually the Ethereum or Solana blockchains which have the requisite protocols for DAOs).[320]

An offer is a 'clear and unambiguous' proposal which outlines the terms under which a party agrees to enter into a contract.[321] The offer occurs at the point where the offeror submits the smart contract to the blockchain.[322] However, given that many DAO smart contract 'offers' are expressed in the form of computer code, it may be questioned whether they constitute offers at all. Code, by its nature, is unclear and ambiguous to many who read it, and therefore may conflict with the requirement that an offer is clear and unambiguous. However, Durovic and Janssen argue computer code alone is sufficiently precise to form the basis of an offer.[323] This is particularly true regarding DAO smart contracts, the target demographic of which will often comprise software designers and technology enthusiasts who may glean the essential terms of the contract from perusing the code. For example, a smart contract could be concluded, which connects a DAO's validators with the DAO's treasury. The validators play a crucial role in upholding the DAO by ensuring the integrity of the transactions that take place upon its network. The code of the smart contract can stipulate the terms under which a user agrees to

[318] Linda Orenes-Lerma, 'What Is a Blockchain Validator?' (*Ledger*, 18 April 2023) <https://www.ledger.com/academy/what-is-a-blockchain-validator> accessed 4 April 2024.
[319] ibid.
[320] 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 71.
[321] McDermott (n 193) para 2.09.
[322] Durovic and Janssen (n 28) 61.
[323] ibid 67.

become a validator. For instance, it can set out the minimum staking amount required before the user is admitted as a validator. This refers to the minimum amount of cryptocurrency that a participant must deposit to become a validator particularly on blockchains which use proof-of-stake consensus mechanisms like Ethereum. Additionally, the smart contract's code may stipulate certain performance criteria such as the amount of uptime required by a particular validator, or that the validator must be based in a certain geographical location to provide further decentralisation. In terms of rewards for a validator, the smart contract may stipulate the amount by which the validator will be remunerated for its efforts such as earning transaction fees or block rewards. Finally, the smart contract may set out penalties which the validator will face should it fail to adhere to the terms set out above. Such penalties are imposed using a slashing mechanism in-built in the smart contract which recognises that a validator has too much downtime and is not fully participating in the upkeep of the DAO, or that it is performing actions in contravention of the DAO's security protocol. When the slashing mechanism is invoked, the validator ceases to receive the rewards promised under the smart contract and will have to pay an amount of Ether for each infringement.[324] All of these terms can be expressed precisely in the form of code in the smart contract which itself will constitute the offer.

Before a contract is validly formed, the offeree must assent to the contract's terms by providing his acceptance. An offeree in a smart contract context can accept a smart contract by using a private cryptographic key or by performing the smart contract's terms.[325] In our example of the DAO and the validator, the validator may accept the smart contract's terms by way of conduct, which involves his payment into the DAO the amount of cryptocurrency stipulated in the smart contract. Additionally, as part of his conduct, he must begin validating transactions on the

[324] Matthieu Saint Olive and Simran Jagdev, 'Understanding Slashing in Ethereum Staking: Its Importance & Consequences' (*Consensys*) <https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences> accessed 12 December 2024.
[325] Durovic and Janssen (n 28) 67–68.

DAO's network. Therefore, there is no reason in theory why the offer and acceptance model of formation should prevent parties from entering legally binding agreements. The courts' analysis will therefore turn on the intentions of the participants within a particular DAO.

However, just because code is a 'precise' way of setting out and executing transactions does automatically enable it to form contracts between parties. A contract involves correlative purposive agents who seek to achieve their self-determined ends. The doctrines of offer and acceptance are a necessary part of the contracting process because they are determinative of a juridical relationship between the parties.[326] Under corrective justice, there cannot be an 'exception' to the rule of offer and acceptance (as Peel suggests) because these acts bring the parties together in a unified transaction. If DAO smart contracts are multilateral contracts, and it is 'impossible or highly artificial' to render them on the basis of offer and acceptance, then this would suggest that DAO smart contracts are not contracts under corrective justice. Instead, they are merely software used to manage the DAO and its participants.[327]

To explain, let us refer back to our earlier example of a DAO transaction involving validators who have an important role in ensuring the integrity of all transactions related to the DAO. The DAO's developers enter a contract with the validators, both of which are connected to the DAO's treasury through a smart contract. The treasury is funded through smart contracts with the DAO's investors. As such, the bilateral nature of contracting breaks down in DAO smart contracts.

[326] Ernest J Weinrib, 'Legal Formalism: On the Immanent Rationality of Law' (1987) 97 Yale Law Journal 949, 962.
[327] Mik, 'The Sense and Nonsense of Smart Contracts' (n 5) 8.

3.8 Consideration in smart contracts

Before proceeding with the discussion of consideration, it is necessary to briefly discuss the value of crypto-assets because consideration must include something of value in the eyes of the law. In this section of the chapter, it is submitted that the doctrine of consideration remains unchallenged by the practice of smart contracting in principle because crypto-assets carry with them legally-ascertainable value. However, the value of crypto-assets is debated. Some argue that cryptocurrencies are only valuable because a 'greater fool' is willing to buy them at a higher price than for what they were initially bought.[328] Crypto-assets are neither tangible assets nor are they currencies as cryptocurrencies lack the status of legal tender.[329] It can be argued that cryptocurrencies have no intrinsic value, and that sceptics are therefore justified in questioning the value of these assets.

However, some value can be identified in cryptocurrencies which would permit them to constitute consideration for the purpose of executing a smart contract. The value obtains from the scarcity of most cryptocurrencies. When a new cryptocurrency is brought to market, it is given a fixed volume where, once reached, no more of that cryptocurrency can be generated.[330] The cryptocurrency generation process, known as 'mining' also provides cryptocurrencies with their value. Cryptocurrency miners use computational resources and their expertise to solve mathematical problems, in return for which they receive a new cryptocurrency which can then be traded.[331]

---

[328] Eswar Prasad, 'The Brutal Truth about Bitcoin' (*Brookings*, 20 July 2021) <https://www.brookings.edu/articles/the-brutal-truth-about-bitcoin/> accessed 14 May 2023.

[329] Matthew Kien-Meng Ly, 'Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies' (2014) 27 Harvard Journal of Law & Technology 587, 589.

[330] Take Bitcoin for example, one of the most popular cryptocurrencies which is valued on a supply and demand basis. According to its whitepaper, a maximum of 21 million Bitcoins can be created, and so there is a finite supply of the cryptocurrency. See Z John Zhang, 'Cryptopricing: Whence Comes the Value for Cryptocurrencies and NFTs?' (2022) 40 International Journal of Research in Marketing 22, 24.

[331] Alex Nicholson, Kingsley Udofa and Alannah Collins, 'Customer Value Theory and Cryptocurrency Regulation' (2022) 3 Journal of Law, Technology and Trust 14.

NFTs are the subject of scepticism for similar reasons as cryptocurrencies. However, the value of NFTs is more apparent than in cryptocurrencies. An NFT's function is to tokenise an asset, often in the form of some digital media such as an image, audio file, video, among others. The value of the NFT therefore derives from the corresponding asset which often includes digital art in which consumers may identify some value.[332] Therefore, crypto-assets may constitute consideration capable of rendering a smart contract as a legally enforceable agreement. Given that £1 may be good consideration, a cryptocurrency traded at approximately €92,000 like Bitcoin will also constitute good consideration. Contract law is concerned with the existence of some exchange and less so with the economic efficiency produced by the transaction. The rationale of the doctrine is to evidence the form of the parties' relationship rather than to scrutinise the imbalance in the values exchanged.[333]

As such, the doctrine of consideration may not prohibit a smart contract from becoming a legally binding agreement. This is because a smart contract cannot be executed without the payment of some consideration into the smart contract, and the consideration must meet the specified value set out in the smart contract before it will be executed.[334] If a smart contract for the sale of a digital image of the Eiffel Tower stipulates a sale price of 1 Ether, the exchange cannot take place until exactly 1 Ether is entered into the smart contract.[335] In sum, there are two aspects to the doctrine of consideration where smart contracts are concerned. Crypto-assets may have exchange value because the broader blockchain community believes in their value. But they may also constitute consideration from the law's view because their exchange may be viewed as a benefit received or a detriment suffered by the parties.

[332] Tuba Yilmaz, Sofie Sagfossen and Carlos Velasco, 'What Makes NFTs Valuable to Consumers? Perceived Value Drivers Associated with NFTs Liking, Purchasing, and Holding' (2023) 165 Journal of Business Research 114056, 9.
[333] Chen-Wishart, 'In Defence of Consideration' (n 177) 233–234.
[334] Durovic and Janssen (n 28) 69.
[335] Ether is a popular cryptocurrency facilitated on the Ethereum blockchain.

3.8.1 Bilateral smart contract consideration

The bilateral smart contract almost certainly does not pose any challenges for the doctrine of consideration. Although the doctrine is complex, two aspects are worth considering in relation to smart contracts. The first, the adequacy and sufficiency of consideration, have already been discussed above, where it was found that crypto assets will typically have exchange value and value in the eyes of the law. The second component to which we now turn our attention is that consideration must move from the promisee. This means that the promisee must have provided some benefit or suffered some detriment in return for the promise, depending on the circumstances of the contract.[336] This aspect of the doctrine has an important role in creating the bilateral relationship between the plaintiff and the defendant because the promisee is required to provide consideration in return for the promise.[337] As such, the interaction is not one-sided, and instead involves both parties undertaking an active role in it.

Under a corrective justice understanding of consideration, there is little difficulty in fitting the bilateral smart contract and the concepts of consideration together. First, there is typically some value to crypto assets in themselves, as well as in the eyes of the law. And second, it is possible for consideration to move from the promisee as it would in a conventional contract. Typically, a smart contract involves the requisite consideration to form a legally binding agreement.[338] For example, Andrew promises (through a natural language agreement) to redesign Noel's e-commerce website to include a homepage, product catalogue, and checkout system. It is also stated in the agreement that Noel will pay Andrew 2 ETH upon the completion and delivery of the new website. Once they have mutually assented to the natural language terms, the parties

[336] Clark (n 182) 82.
[337] Benson, 'The Idea of Consideration' (n 57) 251.
[338] Werbach and Cornell (n 12) 370.

create a smart contract which includes a trigger allowing Noel to confirm that the website is live, thereby paying Andrew. In doing so, consideration in the form of 2 ETH moves from the promisee by way of the smart contract. The software is merely the medium for 'handing over' the asset to the promisor.

The bilateral smart contract hypothetical discussed above involves at its base the exchange of a promise for a promise. Andrew promised to Noel that he would redesign the website, and in return, Noel promised that he would execute the smart contract at a later stage once the work has been completed. Such a return promise is acceptable as Noel still incurs a detriment, even though that detriment is imposed upon him at a later stage (at the point when the smart contract is executed).[339]

In passing consideration to the promisor, the promisee ought to give up something which would be of benefit to him were he to hold on to it, or something which he himself would want to enjoy.[340] The transferral of ETH meets this requirement, given that cryptocurrencies are capable of storing and ascertaining value which may later be traded for something else (even if that value is subject to the volatility of cryptocurrency markets).[341] In sum, bilateral smart contracts may coherently map onto the doctrine of consideration.

3.8.2 DASC consideration

Similarly to the bilateral smart contract, crypto assets have value and will constitute good consideration in DASCs. Instead, the discussion around consideration regarding purely coded contracts concerns the exchange of mutual promises. It is well established that consideration

[339] Benson, 'The Idea of Consideration' (n 57) 253.
[340] ibid 254.
[341] Sarah Green, 'The Meaning of Money' (2020) 44 Brief 12, 17.

may be constituted by mutual promises by the contracting parties.[342] By their nature, the parties' promises concern conduct which they will both undertake in the future. As such, the exchange of promises creates the correlative rights and duties of the parties.[343]

Some scholars have pondered that smart contracts lack the exchange of promises required under the doctrine because of the 'mechanical nature' of smart contracting.[344] Under a DASC, the parties do not communicate promises to one another in a plain language, therefore it is true that there is no promissory exchange involved in the interaction (in the form of a benefit or detriment). In this regard, Werbach and Cornell have conceptualised the smart contract as a process which the parties have no power to stop rather than the exchange of promises or obligations.[345] They stated that the smart contracting process is like placing a bucket of water on top of a door awaiting the next person to enter through it. In this scenario, the placer of the bucket made no promise that the next person will be soaked on entry, but it will certainly occur. In a similar way, a smart contract is a piece of software which, once deployed on the blockchain, exists in a suspended state pending interaction by the offeree. This has led some academics to doubt the presence of consideration in smart contracts because the will of the offeror has been substituted by the autonomous performance of computer code.[346] If this is correct, then it cannot be concluded that DASCs are contracts. Both parties must be interacting as free beings, yet their freedom is restricted if the 'promise' is expressed in code.[347]

However, Giancaspro argues that contract law is 'not particularly concerned with the fact that a string of code, as opposed to the parties themselves, is performing the respective obligations

[342] Edwin Peel, *Treitel's The Law of Contract* (15th edn, Sweet & Maxwell 2020) 82.
[343] Benson, 'The Idea of Consideration' (n 57) 261.
[344] Jasper Verstappen, 'Formation of Contracts' in Jasper Verstappen (ed), *Legal Agreements on Smart Contract Platforms in European Systems of Private Law* (Springer International Publishing 2023) 88 <https://doi.org/10.1007/978-3-031-35407-6_3> accessed 12 December 2024.
[345] Werbach and Cornell (n 12) 340.
[346] Savelyev (n 215) 129.
[347] Weinrib, *Idea* (n 14) 82.

under the agreement.'[348] Smart contracts are, at the least, voluntary mechanisms used to modify the rights and duties of the parties, notwithstanding that they are in code-only form.[349] Although they do not contain mutual promises because computer code is not a promise, consideration may still pass from the promisee in the form of a crypto asset.

3.8.3 DAO consideration

The doctrine of consideration determines the conclusion of a contract between parties because it indicates that the promisee has equally participated in establishing his right to the promisor's performance. By requiring that consideration moves from the promisee, the doctrine ensures the equality of the parties in the transaction because it constitutes a token of the promisee's will.[350] The DAO complicates the movement of consideration by introducing multiple parties through multilateral smart contracting. Consequently, some DAO participants may be left without an enforceable right against other participants, including the DAO's developers. The potential breakdown of any enforceable right occurs because a DAO participant does not provide a benefit or detriment for the 'promise'.

I will conceptualise a hypothetical DAO to demonstrate the point. The DAO's founders create the initial smart contract architecture and deploy its token. Early contributors see the potential of the DAO and offer to develop it further. Third party organisations which align with the DAO's values seek funding through the DAO. Validators (in the form of the DAO's token holders) vote on funding proposals brought by those third-party organisations.

[348] Mark Giancaspro, 'The Consideration Myth about Smart Contracts' (2020) 1 ANU Journal of Law and Technology 35, 37.
[349] Werbach and Cornell (n 12) 341.
[350] Weinrib, *Idea* (n 14) 138.

In this conceptualisation of a DAO, the token purchasers provide consideration to the DAO treasury to obtain tokens, thereby incurring a detriment because they have paid the designated amount of cryptocurrency per token. The early contributors provided a benefit by assisting with the coding of the DAO and obtain tokens in return.

3.9 Intention to create legal relations in smart contracts

The doctrine of intention to create legal relations is the final instantiation of the juridical relationship. Although the doctrines of offer, acceptance, and consideration do most of the heavy lifting, the doctrine of intention to create legal relations has long played an important role in distinguishing binding and non-binding agreements.[351] It is the final filter through which the parties' interaction must pass to determine whether they sought for the arrangement to give rise to legal entitlements.[352] The doctrine may therefore help identify instances where there was no mutual agreement by the parties, the absence of which will be fatal to the parties' corrective justice relationship. If no relationship arises in the first place, then there will be no corrective *in*justice to remedy.

3.9.1 Intention to create legal relations in bilateral smart contracts

Smart contracts are *presumptively* intended to create legal relations where they are used in business-to-business (B2B) or peer-to-peer (P2P) transactions for commercial purposes. The purpose of many smart contracting parties may be to pursue financial objectives. Trade may

[351] See Peter Benson, *Justice in Transactions: A Theory of Contract Law* (Harvard University Press 2019) 117 Benson refers to a standalone doctrine of intention to create legal relations as 'superfluous' because the doctrines of offer, acceptance, and consideration are sufficient for identifying the parties' assent. However, such a debate is beyond the scope of this thesis, and it therefore tests smart contracts against the doctrine of intention to create legal relations because it has long been established in the body of contract law. The doctrine was first adopted into English contract law in *Balfour v Balfour* (1919) 2 KB 571.
[352] *Baird Textile Holdings Ltd v Marks & Spencer plc* [2001] EWCA Civ 274 [59]: 'For a contract to come into existence, there must be … an intention to create legal relations'.

take place within the blockchain community to avoid the perceived overregulation in the offline world. Yet, the transactions will often be commercial in function. One example is that smart contracts are used to lend and borrow for the purpose of trading crypto assets. The use of smart contracts for decentralised finance was highlighted by the facts in *Janesh s/o Rajkumar v Persons Unknown* (‘*Chefpierre’)* where a P2P marketplace, *NFTfi,* enabled its users to collateralise NFT loans.[353] To do this, the borrower transferred an NFT to NFTfi’s escrow smart contract which served as security for the loan. Subsequently, the lenders funds would be transferred to the borrower. The plaintiff placed up an ‘unusually rare’ NFT, an item from the ‘Bored Ape Yacht Club’ collection, as collateral for a loan from the user known only as ‘Chefpierre’. He stated in natural language several extra terms governing the transaction, including that the defendant must not activate the foreclosure option without permitting the plaintiff a reasonable opportunity to fully repay the loan. Additionally, he stated that the defendant in his capacity as lender would not take possession or obtain a right to sell the NFT.[354]

The smart contract in *Janesh* contains elements of both bilateral and DASCs, and fits uneasily within the taxonomy adopted in this thesis. The reason is that the agreement had both coded and natural language elements but the parties did not know each other in an offline capacity. However, since the terms of the smart contract were capable of being negotiated through the marketplace’s user interface, and there was a natural language agreement, the smart contract here is closer to a bilateral smart contract.[355]

Although the issue of intention to create legal relations was not disputed in the case, it illustrates how bilateral smart contracts may be used for commercial purposes. The ends for which each party strives is ultimately financial. The ‘rarity and high value’ of the Bored Ape Yacht Club

[353] *Janesh s/o Rajkumar v Persons Unknown (‘CHEFPIERRE’)* [2022] SGHC 264.
[354] ibid 11.
[355] Timothy Chan and Kelvin FK Low, ‘DeFi Common Sense: Crypto-Backed Lending in Janesh s/o Rajkumar v Unknown Person (“CHEFPIERRE”)’ (2023) 86 Modern Law Review 1278, 1280.

NFT allowed the plaintiff to seek higher loans of cryptocurrency to fund further trading activity.[356] In return, the defendant was due to receive the loan repayment and 45% interest.[357] Therefore, there was a clear commercial purpose underpinning the parties' transaction.

The parties' interaction in this case would constitute a corrective justice relationship, finalised by the doctrine of intention to create legal relations (had it been applied by the Court).[358] This was evident when the plaintiff stated that the defendant ought not to exercise the foreclose option on the smart contract, and the defendant assented. The loan agreement was for 150,000 DAI cryptocurrency which at the time equalled approximately $150,000 USD, and had a duration of 30 days with an interest payable at 45% per annum.[359] These were the terms to which both parties agreed to be bound, which had an obvious commercial rationale. And notwithstanding that both parties had communicated using natural language prior to the execution of the smart contract, neither party disclaimed intention to create legal relations.

While it is argued here that bilateral smart contracts, like that in *Janesh*, will often include an intention to create legal relations, it is argued in the next section that DASCs may also include the requisite intention.

3.9.2 Intention to create legal relations in DASCs

DASCs may also be used to facilitate commercial transactions, however the parties who use them may disclaim any intention to create legal relations at all. Disputes about intention often

[356] *Janesh s/o Rajkumar v Persons Unknown ('CHEFPIERRE')* (n 326) [10].
[357] ibid 17.
[358] Like many judgments related to crypto-assets published at the time of writing, the judgment in *Janesh* only concerned preliminary matters.
[359] *Janesh s/o Rajkumar v Persons Unknown ('CHEFPIERRE')* (n 326) [17].

arise from vague or informal interactions, but smart contracts are precise, and are often commercial in their purpose.[360]

If it is found that such an intention is absent in the parties' interaction, a contract is not formed and the courts will be unable to rectify any normative losses incurred by the plaintiff.[361] And it may be the case that some DASCs are made without such an intention. For example, the lack of intention in smart contracts has been identified by certain legal scholars who have argued that smart contracts are not legal agreements, but computer programmes used to manage digital assets. For example, Fairfield argued that autonomous software may not constitute a contract where there is a lack of intention to create legal relations or an exchange of promises.[362] DASCs typically do not feature interactions between the parties except the execution of computer code. If this form of smart contract is simply code, than any expression of the parties' mutual intentions is buried in the code, if it exists at all. It is important to remember that smart contracts were supposed to be an alternative to the legal system, and that parties do not have to assume contract's laws advantages and constraints.[363] Stated another way, parties may not wish to enforce smart contracts because performance of the smart contract is automated and therefore should not require court-based enforcement in the future.

Whether a smart contract satisfies the requirements of the intention to create legal relations doctrine will depend on its composition. Corrective justice is concerned with the 'externally recognisable acts' of contracting parties, therefore the focus will be on whether the parties had conducted themselves in a way that would lead the courts to believe that an intention to create

[360] A notable recent case on intention to create legal relations in informal contexts is *Blue v Ashley* [2017] EWHC 1928 (Comm); Sarah Green and Adam Sanitt, 'The Contents of Commercial Contracts: Smart Contracts' in Paul S Davies and Magda Raczynka (eds), *Contents of Commercial Contracts: Terms Affecting Freedoms* (Bloomsbury Publishing 2020) 199

[361] Roger Brownsword, 'Automated Transactions and the Law of Contract: When Codes Are Not Congruent' in Michael Furmston (ed), *The Future of the Law of Contract* (Informa Law 2020) 102.

[362] Joshua AT Fairfield, 'Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property' (2022) 97 Indiana Law Journal 1261, 1286.

[363] Green and Sanitt (n 360) 9.

legal relations did arise.[364] If the offer is intelligible to human-readers, then it may be easier to discern whether its parties objectively had intended to enter a legally enforceable agreement.[365] A reasonable person may then consider the smart contract to be binding particularly where it is used in a commercial context.[366] Especially, the courts may find following an objective assessment of the agreement that the smart contract was used as part of a commercial transaction with an underlying intention to be bound, even if such an intention was not expressly stated.

It is therefore likely that a majority of DASCs will satisfy the requirement that the parties intended to be bound by the agreement. They will often be used to exchange some form of digital asset for another digital asset. The most predictable example is the exchange of one cryptocurrency for another, or the sale and purchase of an NFT. These assets are typically purchased as a form of investment, therefore an underlying commercial purpose may be identified.[367]

3.9.3 Intention to create legal relations in DAOs

DAOs can be divided into separate categories based on their underlying purpose. Whether or not the parties intended to create legal relations will depend on that purpose, because it may be considered a commercial arrangement, or it could be considered a social arrangement. The former class of arrangement has attached to it a rebuttable presumption that the parties intended to create legal relations, while the latter tends to lack that intent.[368] If it is apparent that the

[364] Weinrib, *Idea* (n 14) 104.
[365] Durovic and Janssen (n 28) 71.
[366] *Hadley v Kemp* [1999] EMLR 589.
[367] Marco Di Maggio and Ben Rand, '"Not a Bunch of Weirdos": Why Mainstream Investors Buy Crypto' (*Harvard Business School*, 17 August 2023) <https://www.library.hbs.edu/working-knowledge/not-a-bunch-of-weirdos-why-mainstream-investors-buy-crypto> accessed 14 September 2023.
[368] Peel (n 308) 193.

DAO was created without an intention to create legal relations, then there will be no contract upon which the parties may claim that they have suffered any loss.

Some DAOs exist as social organisations where participants purchase the native crypto-token merely as a means to access the digital community.[369] For example, BookDAO serves as a hub for co-authors to collaborate and organise their ideas with one another.[370] To gain access, new members must buy an NFT which allows them to authenticate and access the DAO. Without some underlying commercial objective to the DAO, the interactions that occur internally and externally to that DAO may not be contractually enforceable because there is no presumption of any intention to do so.

Hypothetically, the DAO may run occasional competitions for best written works to incentivise collaboration and the completion of books. The prize could be in the form of a tokenised graphic of a trophy. However, if the DAO failed to provide the prize, it is unlikely that the winners could successfully sue to receive it. For instance, the winner of a competition was unsuccessful in suing a golf club which held the competition because the participants objectively never intended that legal consequences would flow from the terms and conditions of the competition.[371] Given that BookDAO's function is a social forum for participant authors to meet other authors, it would be unlikely that the courts would identify any intention to create legal relations between the various authors and the DAO. It is therefore necessary to look to the purpose for which the individual DAO was created unless the parties have shown an express intention to create legal relations.

Many DAOs are commercial in their nature, and therefore the courts may be more willing to presume that the parties therefore had intended to create legal relations. In *Hadley v Kemp* for

[369] 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 15.
[370] 'Book DAO Co-Author Collective' <https://www.bookdao.org/> accessed 14 December 2024.
[371] *Lens v Devonshire Club* (1914) (The Times), discussed in Peel (n 308) 193.

example, Park J. stated that contracts formed in the commercial context often are presumed by the courts to be legally binding.[372] One type of potentially commercial DAO is the investment DAO which is used by participants to pool funds together with a view to invest into other forms of cryptocurrencies.[373] The profits received into the DAO may then be distributed to each participant based on their contribution to the fund. Given that the parties here are driven by their desire to gain profit through crypto-investment, they may wish to be safeguarded through the creation of contractual rights. The relationship between the participants here then is commercial rather than social.

However, participants in an investment DAO which takes the form of a 'pure DAO' may argue against the creation of legal relations. Generally, members of various blockchain communities may resist legal or technical intervention because it would undermine the immutability principle of the blockchain, therefore eroding confidence in the overall system.[374] In their view, the blockchain is supposed to act as an alternative to legal enforcement. However, these users are not representative of all blockchain users who may in fact intend for their smart contracts to establish legal relations. These contrasting positions are demonstrated by the investment fund *TheDAO* discussed earlier which disclaimed the creation of any legal relations between its members.[375] However, the test for intention is objective and therefore it is irrelevant that particular parties to a DAO believed or did not believe such intention existed.[376] As such, the commercial nature of the agreement involved here would give rise to the presumption of such an intention, notwithstanding *TheDAO*'s claims to the contrary.[377] The DAO's participants may try rebut the presumption, but the onus is a heavy one and therefore they may be unsuccessful

[372] *Hadley v Kemp* [1999] EMLR 589, 624.
[373] 'Decentralised Autonomous Organisations Scoping Paper' (n 240) 15.
[374] Mark Verstraete, 'The Stakes of Smart Contracts' (2018) 50 Loyola University Chicago Law Journal 743, 777.
[375] Andrew M Hinkes, 'The Limits of Code Deference Symposium: The 20/20 Vision: Blockchain and the Future of Law' (2020) 46 Journal of Corporation Law 869, 883.
[376] *Albert v Motor Insurer's Bureau* (1971) 2 All ER 1345.
[377] *Esso Petroleum Ltd v Commissioners of Customs and Excise* [1975] UKHL 4; Durovic and Janssen (n 28) 71.

in their attempts.[378] Given the significant sums of money involved in many DAO projects, it is best that the courts presume an intention existed unless it can be shown that participants to a particular DAO objectively did not seek to create a contractual relationship. This way, they may be able to recover for losses that might arise resulting from the DAO's activities.

3.10 Conclusion

Smart contracts are legal contracts where the requisite conditions exist. This chapter has examined the doctrines of contract law concerned with contract formation and found that a valid offer and acceptance may be found in certain smart contracts. It further found that the doctrine of consideration is unimpeded by smart contracts as a smart contract requires valid consideration before it can be executed. It is the consideration that activates the smart contract, without which the transaction will not occur. As such, smart contract transactions of all types will usually involve the transferal of a 'token of the will' that signals the offeree's willingness to be bound by the agreement. Finally, on the point of intention to create legal relations, smart contracts facilitate significant commercial transactions for which the protection of contract law is desirable. Of course, parties may rebut the presumption that a given smart contract was intended to create legal relations, however this chapter argued that most smart contracts are inherently commercial contractual devices and as such should be enforced by the courts. There will of course be exceptions which I have highlighted by reference to 'social DAOs' where the purpose is not profit but community. This chapter established that some smart contracts may in fact be legal contracts, and may better satisfy the criteria of corrective justice. The following chapter analyses how smart contracts may be interpreted depending on whether or not they are accompanied by a natural language document.

[378] *Edwards v Skyways Ltd* [1964] 2 WLR 349, 355.

4 From Paper to Protocol: Interpreting Smart Contracts Under Traditional Contract Law

4.1 Introduction

The interpretation of agreements in the digital era is no longer exclusively within the remit of lawyers. For decades, the courts have tried to determine the best approach for interpreting contracts, moving between contextualist and literalist positions at various periods.[379] Yet, one commonality between both positions is their focus on words, although the importance of the words is weighed differently by the different approaches. For instance, the literalist approach places emphasis on the words as they are enshrined in the written agreement, and the courts did not tend to deviate from the dictionary definition of those words. Then, the courts adopted the contextualist approach in which the words were given effect by reference to the surrounding context of the agreement. Nonetheless, the courts at least had words to grasp, to interpret. Moving into the technological era, words are much less a prerequisite for agreements and now, computer code will suffice to make legally binding agreements. Parties may instead opt to use programming language to form the terms of the contract.[380] Smart contracts, some might argue, eliminate the need for interpretation because code is sufficiently precise and cannot have more than one meaning.[381] Although many agreements will continue to be made through the classic method of ink, paper, and natural language, many parties will opt for algorithmic programmes to enforce their bargains. If this is the case, then how appropriate is legal doctrine that has been

[379] Rónán R Condon, 'After Law Society v MIBI: Contextualism and Contracting in Irish Contract Law' (2019) 62 Irish Jurist 51.
[380] Rizos (n 175) 793.
[381] Michel Cannarsa, 'Interpretation of Contracts and Smart Contracts: Smart Interpretation or Interpretation of Smart Contracts?' (2018) 26 European Review of Private Law 778.

developed at a time when parties simply used a numbered list of terms and conditions? After all, it will be difficult to determine what the parties intended by looking solely at lines of code.

If a contract cannot be interpreted beyond its code, corrective justice may find it difficult to rebalance the parties' holdings in a way that corrects any injustices. In a DASC or DAO for example, the context of the smart contract may be limited to the content of the smart contract itself (that is, its code). Otherwise, the courts may look to the purpose for which the DAO was established to determine the reason for the parties' interaction. However, if it is the case that there are no alternative outward expressions of the parties' manifested will, the harmed party may have to bear their losses. On the other hand, the courts may refer to the parties' written agreement and the factual matrix that may be established around bilateral smart contract arrangements.

4.2 Principles of interpretation

Courts may have difficulty interpreting smart contracts expressed entirely in software code.[382] Traditionally, they have used a literal approach to ascertain the meaning of the contract in which they would assess the words used based on their dictionary definition. Since then however, they have adopted a contextualist approach where they may draw on evidence external to the contract to determine the objective intentions of the parties. The criteria for interpretation were set out by the House of Lords in *Investors Compensation Scheme Ltd v West Bromwich Building Society*.[383] In that case, the Court held that the meaning of the contract is determined by reference to how a reasonable person would understand it, with all relevant knowledge that the parties had at the time of entering the agreement.[384] The background (or the matrix of fact)

[382] Green, 'Smart Contracts, Interpretation and Rectification' (n 160) 245.
[383] *Investors Compensation Scheme Ltd v West Bromwich Building Society* [1998] 1 WLR 896.
[384] ibid, 912.

includes anything which presumably forms part of the deal. This includes anything except utterances made during prior negotiations.[385]

The majority of the Irish Supreme Court in *Law Society of Ireland v Motor Insurers' Bureau of Ireland* also favoured the contextual approach to contract interpretation.[386] Under its approach, the principle that contracts should be understood according to their plain meaning has been reduced to a 'rule of thumb'.[387] External factors must also be considered such as the broader context of the transaction, the applicable law, the other terms contained in the agreement, any prior agreements entered into by the parties, and the logic of the agreement.[388]

Contractual interpretation has an important role in ensuring corrective justice because it involves an assessment of the terms which bind the parties together in a unified interaction. The relationship of the parties is constituted by their mutual connection to one another.[389] Part of this unity may be whether they had a shared consensus for the contract. The doctrine of interpretation seeks to determine the meaning of the contract used by the parties according to a reasonable person's comprehension of the words used.[390] The objective approach is adopted because 'contract cannot be held hostage to the vagaries of a private intention'.[391] Therefore, the courts may, and do, take into account the outward actions of the parties which may determine what they sought to achieve from their mutual connection.

In undertaking the interpretative exercise, the courts seek to identify the true agreement between the parties rather than re-writing the contract for them. Ordinarily, the content of the parties' agreement was found within the four corners of the paper contract and extrinsic evidence could not be relied upon to define the contract's purpose. Under the contemporary

[385] ibid, 913.
[386] *Law Society of Ireland v Motor Insurers' Bureau of Ireland* [2017] IESC 31.
[387] Condon (n 379) 60.
[388] *Law Society of Ireland v Motor Insurers' Bureau of Ireland* [2017] IESC 31 [12].
[389] Weinrib, *Idea* (n 14) 35.
[390] Ryan Catterwell, 'Automation in Contract Interpretation*' (2020) 12 Law, Innovation and Technology 81, 83.
[391] Weinrib, *Idea* (n 14) 104.

position, the courts attempt to place themselves in the position of the parties by accessing the same factual matrix to which the parties were privy at the time the contract was concluded.

Given that a contract is the manifestation of the free will of its parties, the courts ought to identify the right and duty created under the contract and enforce it accordingly.[392] Under corrective justice, the parties are entitled to order their relations as they deem appropriate. The courts are more concerned with what the parties objectively agreed rather than the economic efficiency of their agreement. Although, the courts in business contracts base their analysis on the 'commercial sensibility' of the transaction – an approach which may have a functionalist hue. However, Lord Steyn stated that the reason for this approach is that appraising a business contract through a commercial lens may more accurately give effect to the parties' intentions.[393] The commercial sensibility approach therefore helps the courts ascertain the objective meaning of the contract.

The different modes of interpretation offer distinct ways of obtaining the parties' rights and duties, both with respective advantages and disadvantages. A strict textual analysis ensures a predictable and certain outcome for the parties because the words contained in the document determine the contract's meaning.[394] However, many utterances are understood according to the recipients' shared understanding of both the words used, and the context of the utterances. Contracting is no exception. Therefore, the rights and duties of the parties are best ascertained by considering the contextual clues available to the courts. As will be argued however, context may not play a significant role in decentralised autonomous smart contracts, although coded

[392] ibid 106.
[393] *Mannai Investment Co Ltd v Eagle Star Life Assurance Ltd* [1997] AC 749, 771.
[394] Lord Sumption, 'A Question of Taste: The Supreme Court and the Interpretation of Contracts' (2017) 17 Oxford University Commonwealth Law Journal 301, 309 (criticising contextualist interpretation because it discounts the value of words as a means to communicate party intentions).

agreements without plain language documents do not exist in a transactional vacuum, and therefore context will factor – perhaps in a lesser way than it would in bilateral smart contracts.

The coded agreement requires specificity to ensure the contract is performed as intended by both parties. Nonetheless, the factual matrix of the smart contract may include the written agreement that accompanies the coded agreement. At this point, it is necessary to clarify what exactly is the contract. Parties might regard the smart contract code as the whole agreement, and use the written agreement merely to define those terms in a way which is comprehendible to any potential readers.[395] Alternatively, the parties may treat both the smart contract and the written agreement as constituent parts of the overall agreement. In the latter type of agreement, the parties could include an express reference to the written agreement in the smart contract.[396] Otherwise, they could include an 'entire agreement' clause which states that the smart contract solely governs the agreement, and that the written agreement is merely to help the parties understand the smart contract's contents.[397] In other words, the agreement may be formed using both a smart contract and a written agreement, or just a smart contract. The difficulty with interpretation and fit arises particularly in the latter scenario.[398]

4.3 Interpreting Parallel Agreements: The Smart Contract and Natural Language Document

The purpose of the smart contract in a bilateral smart contracting scenario is to automate the performance of an agreement which is formed off-chain.[399] Under this model of smart

[395] For example, to assist offerees who are unfamiliar with computer code. As crypto transactions became more popular, it was sensible to make smart contracts comprehendible to non-coders.
[396] Jenny Cieplak and Simon Leefatt, 'Smart Contracts: A Smart Way to Automate Performance Technology Explainers' (2016) 1 Georgetown Law Technology Review 417, 418.
[397] Peel (n 308) 234.
[398] This difficulty is later examined in Section 2.6.1.
[399] Filatova (n 19) 239.

contracting, the parties begin by formulating the terms of their agreement through negotiations that are typical of traditional contracting. Once they have agreed on the terms of the transaction, they code those terms into the smart contract so that they are automatically executed and the result is recorded on the blockchain. The process of constructing the terms of a smart contract is more difficult than constructing those of a conventional contract because of the rigidity of computer code.[400] However, this is mostly unproblematic in bilateral smart contracts because the courts will simply have to look to the plain language document to ascertain the intentions of the parties. The issue that does arise however, is that the computer code may not always reflect the parties' intentions. The role of the courts therefore will involve scrutinising the conventional document and comparing its words with the outcome of the smart contract's code.

In particular, the courts might have to interpret a bilateral smart contract transaction in which the offer contains an ambiguity.[401] Allen argues that, if a smart contract's code is successfully executed, then it does not contain any inherent ambiguity because the computer was capable of understanding its terms.[402] This is true as smart contracts are written in 'dry code' which can only have one meaning, and not multiple meanings as do conventional, natural language documents.[403] However, ambiguities may still arise where the transaction begins with a plain language agreement followed by a smart contract, but such a contract is more amenable to interpretation by the courts than a code-only contract.

For example, Party A, a cryptocurrency trader, may seek to borrow stablecoins from Party B, a decentralised financial lending protocol. To do so, he provides some of his own

[400] Green, 'Smart Contracts, Interpretation and Rectification' (n 160) 240.
[401] Collins (n 167) 232.
[402] This position applies more accurately to DASCs which will be assessed later in this chapter. However, where the parties prioritised a natural language document, it matters less how the code performed independently of the written agreement. *See* Allen (n 4) 50.
[403] Michel Cannarsa, 'Contract Interpretation' in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019) 106; On the ambiguities contained in contracts and how courts resolve them, *see* Catherine Mitchell, *Interpretation of Contracts* (Routledge-Cavendish 2007) 40–41.

cryptocurrency as collateral. A plain language explanatory document which forms part of the smart contract stack sets out the terms of the transaction. It states that Party A's collateral will be automatically liquidated if its value falls below a 150% collateralisation ratio. This ratio is determined using an oracle which fetches data from three exchanges to determine the fair market price. The document also states that if an exchange suffers a malfunction or exhibits prices not representative of the state of the market, then its data will be excluded from the calculation. Due to a temporary error, one of the exchanges incorrectly shows a 90% price drop, and the smart contract liquidates the trader's cryptocurrency because the median of the three exchanges falls below the collateralisation ratio.

Party B might argue that the smart contract's code was the final agreement and that the explanatory document is merely non-binding guidance, and that the code performed as designed, and Party A accepted the risk when executing the smart contract. Further, Party B might argue that the document did not include an explicit obligation to override the code, and that without a coded mechanism to exclude data anomalies, the liquidation was valid under the terms of the contract. Whether Party B is correct should be determined by referencing the plain language agreement because it formed the basis for the parties' transaction. The will of the parties is identifiable by looking at the words contained in that document rather than inspecting the code of the smart contract.

When the courts interpret the smart contract, they aim to identify how the parties sought to voluntarily affect change to their pre-existing legal relationship. Corrective justice is centred on the correlative right of the plaintiff and the duty of the defendant, enabling the parties to contract upon the grounds which they consider appropriate for their needs.[404] The reciprocal rights and duties of the parties are expressed through the written agreement. The courts may

[404] See discussion in section 2.4.2.

therefore draw upon the written document to determine how the parties voluntarily affected change to their pre-existing legal relationship.

The smart contract may offer the courts insight into the intentions of the parties involved, and thus may constitute a component of the factual matrix, but most weight will be given to the natural language document. The question then is how a reasonable person would understand the contract, taking into account the transaction in its entirety. It is likely that a reasonable person would find that the parties intended that incorrect data would not be used in calculating the market value. Therefore, Party B made a wrongful gain by retaining the collateral of Party A, and the equilibrium of the transaction must be restored.

In navigating bilateral smart contracts, it becomes apparent that while automation offers efficiency, it must not eclipse the foundational principles of contract interpretation. The interplay between computer code and plain language serves as a reminder that clarity in the parties' intentions is paramount. In interpreting smart contract stacks, the courts must scrutinise the written agreements, ensuring that the true will of the parties is preserved in technologically executed agreements. The challenge for the courts lies in harmonising the precision of code with the nuance of human understanding. However, it becomes difficult to ascertain the will of the parties when they have only used a coded agreement to alter their rights and duties.

4.4 Interpreting Code: Smart Contracts in Isolation

When parties draft a conventional contract, they begin by forming their intentions and expectations in the abstract. Once this initial stage is completed, the parties (or their lawyers) translate those intentions into words which are then included in the contract.[405]

[405] Eric Tjong Tjin Tai, 'Smart Contracts as Execution Instead of Expression' in JG Allen (ed), *Smart Legal Contracts: Computable Law in Theory and Practice* (Oxford University Press 2022) 276–277.

When they engage in contractual interpretation, the courts first ascertain the parties' intentions in the plain language document.[406] Without a plain language document, the courts' decision will draw predominantly on the smart contract's code, and if necessary, the surrounding context of the transaction. Traditionally, interpretation involves examining the usage of words and the syntax of sentences contained in the contract to objectively determine its meaning. Parties sometimes use the wrong words or syntax, in which case, the context of the contract increases in significance.[407] Syntax is more essential in computer code than it is in natural language. Programming languages have strict rules around their allowed inputs, and the order in which they are entered into the software's code. If a coder does not adhere to the formal rules of a given programming language, the software application will not perform as intended. In computer code, there is little room for ambiguity like that which exists in natural language.[408] Therefore, if a DASC is disputed, the courts may have to draw upon the minimal context available to them to determine the will of the parties.

Although the contextual approach permits the courts to draw upon the surrounding context of the transaction, the normal meaning of words still forms part of the factual matrix. In this regard, Keane J. stated in *LAC Minerals v Chevron* that unambiguous contracts 'can only have one meaning' which 'the court cannot go beyond that unambiguous meaning so as to seek to interpret the intention of the parties'.[409] Computer code in isolation cannot contain ambiguities unlike natural language. Software generally, and smart contracts particularly, require accurate input to generate intelligible output. If a line or a block of code is absent from the programme's codebase, it will not perform at all, or its performance will be messy. For this reason, standalone smart contracts purportedly do not require, or permit, interpretation by the courts.[410] In other

[406] Cannarsa (n 229) 108.
[407] *Law Society of Ireland v Motor Insurers' Bureau of Ireland* [2017] IESC 31, para 9.
[408] Mik, 'Contracts in Code?' (n 170) 483.
[409] *LAC Minerals v Chevron* (6 August 1993, HC) 28–29.
[410] Cannarsa (n 381) 781.

words, smart contracts represent a shift back to the literalist interpretative approach where the contents of a contract are ascertained within the four corners of the agreement.

However, the way in which code functions may lead to injustices because of the computer's means of comprehension. For instance, a computer may be instructed to 'go to the shop and buy a newspaper. If there are any eggs, get a dozen', its user will likely be provided with twelve newspapers and zero eggs.[411] Under a human's understanding of the same statement, the context of the arrangement would consider it unusual for someone to seek a dozen newspapers based on the precondition that the shop stocks eggs. Computer code may therefore result in absurdities for which parties may seek clarification from the courts.

However, smart contracts do not facilitate the interpretive contextualism used by the courts to determine the meaning of conventional contracts. The reason is that smart contracts have an 'automated execution chain' where humans are not required to interpret the contents of the contract.[412] Performance takes place in the form which is provided for in the code, and it does not matter how the human parties perceive the code. This is particularly the case where the code is finalised by two algorithms communicating with one another to conclude the terms of the parties' interaction.[413]

Evidently, in DASCs, the parties are prevented from interpreting the smart contract's terms because its execution occurs spontaneously upon its acceptance. In this regard, the code of the smart contract must only be comprehended by the computer responsible for its execution.[414] And the computer disregards the human understanding of particular terms or words – it

[411] Example by Sarah Green. *See* Green, 'Smart Contracts, Interpretation and Rectification' (n 160) 245.
[412] Tjong Tjin Tai (n 378) 278.
[413] To clarify, the party or parties write the smart contract which operates deterministically. They write some of the code and include the parameters of their desired outcome. To finally execute the transaction, their code will have to be concluded with the final price reached by the parties' respective algorithms. See May Fong Cheong and Mimi Zou, 'Resolving Wrongs in Algorithmic Contracting: Applications of the Doctrines of Unconscionability' (2025) 48(4) University of New South Wales Law Journal (Forthcoming)' (Social Science Research Network, 1 July 2025) 8 <https://papers.ssrn.com/abstract=5337542> accessed 10 July 2025.
[414] Tjong Tjin Tai (n 378) 278.

operates according to its own understanding of the programming language used to form the contract. As such, DASCs are not open to interpretation in the same way as are bilateral smart contracts. Code alone has no meaning and only serves as an instruction to a computer to undertake a particular course of action.[415]

It follows that the DASC cannot be interpreted according to the corrective justice standard. Corrective justice centres on the 'transactional equality' of the parties and considers factors that are relevant to them both.[416] Under corrective justice theory, the factual matrix would involve anything that the parties reasonably expected would affect their mutual understanding of their unified interaction. The commercial sensibility test may be used by the courts to strive toward a meaning of the contract on which the parties may be said to agree. Such tests are useful in the realm of traditional contracting, and in construing the written document in a bilateral smart contract. However, these maxims are obsolete in decentralised anonymous smart contracting. Interpretation only aids the courts and the parties to understand the code and how it will execute, but they lack the ability to determine how it *should* execute.[417] Even if the code of the smart contract upsets the transactional equilibrium between the parties and one party disputes the meaning of the smart contract, the courts are not in a place to interfere with the way the code executes.

One example where the code performed as written but likely did not reflect the mutual will of the parties was *Quoine Pte Ltd v B2C2 Ltd*.[418] The transaction in this case materialised due to an error in the code which did not fully prevent the smart contract's performance, but it affected the outcome in a manner which Quoine did not intend. It showed that, among other things, code can be an ineffective method for expressing the parties' will because it does not provide

[415] ibid 279.
[416] Ernest J Weinrib, 'The Jurisprudence of Corrective Justice', *Clarendon Law Lectures* 13 <https://docs.law.utoronto.ca/nawplt3/papers/ErnestWeinrib.pdf> accessed 11 August 2025.
[417] Tjong Tjin Tai (n 378) 280.
[418] *Quoine Pte Ltd v B2C2 Ltd* (n 216).

the same level of detail as a natural language agreement. Thus the textual document, if it exists, should be prioritised over the code. Often times, the code itself will include comments which indicate the function of particular lines of the code.[419] If these are present in the code, and are visible to both parties, then it becomes easier to interpret the contract because they provide some facts other than the code upon which the courts can draw. If they are absent, we return to a position where code is an inadequate means for expressing the will of the parties that may bind them in a unified manner.

4.4.1 Interpreting DAO smart contracts

The 2016 'DAO Hack' was another example of a code-produced absurdity where those involved had opposing interpretations of the terms of the interaction. The purpose of the DAO was to invest in early-stage technology projects, and its participants were entitled to vote on the projects to receive funding.[420] One of the DAO's smart contracts contained a bug which neither its coders nor its reviewers identified. The smart contract which contained the bug existed to enable investors in the DAO to exit the scheme, and in doing so, withdraw their investment.[421] However, the bug allowed the attacker to execute the same piece of code multiple times, contrary to the intended one time.[422] In doing so, they withdrew approximately $60 million worth of Ether from the funds invested in the DAO. The attacker, among others, argued that the withdrawal of the Ether was valid because the smart contract permitted it (based on the 'code is law' principle), while a cohort of the community argued the transaction was illegitimate and ought to be reversed. Ultimately, the issue was resolved technologically (by

[419] Shaanan Cohney and David A Hoffman, 'Transactional Scripts in Contract Stacks' (2020) 105 Minnesota Law Review 319, 367.
[420] Wright (n 313) 159.
[421] Dammers (n 280) 36.
[422] Maarten Everts and Frank Muller, 'Will That Smart Contract Really Do What You Expect It To Do?' (TNO) 10 <https://nn8.nl/publications/pdfs/Everts2018WTS.pdf> accessed 5 June 2023.

way of a 'hard fork') rather than relying on any legal procedure. However, the scenario demonstrates how strict deference to the performance of computer code may result in injustices. How would the courts interpret the smart contract in this dispute?

DAOs (and *TheDAO* is no exception) may be constituted by a web of multilateral smart contracts. The difficulty lies in ascertaining the rights and duties of the parties of the DAO. Had the problematic smart contract been disputed, could the doctrine of interpretation ensure fairness (i.e. by identifying the common intensions of the parties) so as to bring about corrective justice? The likely answer is negative.

The courts may ascertain party intention by placing themselves in the parties' position at the time the smart contracts were created, taking into account the same facts that were available to the parties.[423] However, the DAO smart contract encounters similar issues to the DASC but on a greater scale. For instance, the smart contract which permitted the withdrawal of US$60 million of Ether existed within the nexus of other smart contracts which constituted the DAO. Although these other smart contracts could be factored into the factual matrix, they may be equally indeterminate of the parties' intentions. The reason is that there is little room for interpretation. The meaning of the code is understood by running it rather than by reading it.[424] While this maxim may apply to coded agreements generally, its application is more pertinent with respect to DAO smart contracts.

Such smart contracts are used to manage the governance and assets of the DAO rather than to expressly create a unified relationship between participants. DAO smart contracts are difficult to interpret because they exist within the nexus of smart contracts that constitute the DAO. This means that to interpret the impugned smart contract may require that the courts draw on the smart contracts within the web. Each smart contract added to the nexus increases the

[423] *Staffordshire AHA v South Staffordshire Waterworks Co* [1978] 3 All ER 769, 775.
[424] Green and Sanitt (n 360) 10.

complexity of the smart contract and the ability to scrutinise its code within its overall context.[425] Given that many of these smart contracts will be in code-form only, trying to interpret them may be a futile task. Particularly, DAOs may resist the interpretation of their smart contracts because an amendment to one smart contract may have knock-on consequences for the rest of the network.

However, in the matter of the 'theDAO' hack, its founders and community sought a fair outcome by voting for and exercising a hard fork. Had the smart contract been interpreted by the courts, they may take into account the context of the overall DAO as a vehicle for investing in other blockchain projects. From the standpoint of commercial sense, it is apparent that the DAO's founders did not intend that any participant could withdraw more than the value of their own investment. Although a portion of the community argued that the withdrawer had simply relied upon the terms of the contract contained in code, such a claim may only succeed if the courts interpreted the agreement formalistically.[426] The broader context in which the agreement is situated may determine a fair interpretation of same. This context, if necessary, may include the other coded constituent parts of the DAO which may indicate the function of the given smart contract.

4.5 Conclusion

Smart contracts challenge the rules of contract interpretation. Computer code is held by some as being sufficiently precise so as not to warrant interpretation at all. Notwithstanding its purported predictability and the automation it affords, coded agreements can also result in

[425] TJ de Graaf, 'From Old to New: From Internet to Smart Contracts and from People to Smart Contracts' (2019) 35 Computer Law and Security Review 105322, 10.
[426] Adam J Kolber, 'Not-So-Smart Blockchain Contracts and Artificial Responsibility' (2018) 21 Stanford Technology Law Review 198, 201–202 ['A rupture formed in the Ethereum community. Some denounced proposed remedies, arguing that the alleged hacker simply took advantage of contractual terms, in the form of computer code, to which all investors in TheDAO had agreed.'].

outcomes that diverge from the mutual intentions of the parties. Under the established regime of interpretation, the courts draw on the broader context of the parties' agreement rather than finding its terms within the four corners of the document. In cases where a plain language document accompanies the code, it will often serve as the primary reference point for determining the mutual will of the parties.

However, when agreements exist only in the form of code, the courts must grapple with the limitations of programming languages, which may not capture the nuance and flexibility of human comprehension. Disputes such as the DAO hack and *Quoine* show that treating the code as the contract may produce results that conflict with parties' expectations and the requirements of corrective justice. The courts must therefore balance the technical execution of smart contracts with their contextual basis, and the parties' intentions which underpin pin. Ultimately, the courts may better safeguard the integrity of parties' agreements by drawing on their surrounding context. This way, the courts can uphold the fundamental idea that contracts are, above all, expressions of the parties' mutual will, and not the performance of code in the abstract.

5 Voiding the Digital Deal?: Assessing the Smart Contract for Vitiation

5.1 Introduction

The previous chapters discussed how the corrective justice theory determines when a smart contract may be an enforceable legal agreement and when it might not. Corrective justice also explains why a contract may be rescinded or unenforceable. Fundamentally, contracts are entered into by self-determined and equal agents who determine their own purposes through contracting. The agent's equality may be impeded by a vitiating factor, meaning that she based her determination on something which did not accurately reflect the contract into which she had entered.[427] A correctively unjust transaction occurs when a 'defendant who breaches that equality realizes a gain solely in the sense of having more than he or she ought to have as a matter of corrective justice'.[428] From here, a corrective justice account of the vitiating doctrines can be formed. A defendant gains more than what he ought to have if the plaintiff transacts on account of a mistake or misrepresentation, due to which he entered a transaction which he would not have ordinarily entered.

Two instances of potential vitiation are already apparent across smart contract transactions. The first to be examined here is occurrences of mistake which may occur in two distinct ways. In a bilateral smart contract, the terms of the agreement are set out in a natural language document. The mistake arises where discrepancies exist between the rights and duties established in the plain language agreement and how the code of the smart contract performs those terms. Where the parties have not expressly accounted for the risk of errors contained in the smart contract

[427] Michael Bryan, 'Justice Callinan's Judgments in Private Law: Story Telling, Legal Coherence and Corrective Justice' (2008) 27 University of Queensland Law Journal 29, 36.
[428] Weinrib, 'Corrective Justice in a Nutshell' (n 13) 354–355.

in natural language terms, it is to the doctrine of mistake which they might turn.[429] Alternatively and more complicatedly, DASCs lead to mistakes where their terms are 'negotiated' by algorithms with minimal human input. And whether corrective justice should require that the courts unwind a transaction exercised by algorithms is a source of debate.[430] Ultimately there are two reasons favouring judicial intervention. First, that there was no contract at all because DASCs may not be contracts. And second, DASCs sometimes use black box algorithms to negotiate the terms of transactions, therefore offerees may not fully understand what it is they are receiving as part of the interaction. In such an instance, is it possible to say that the plaintiff acted with equal freedom to the offeror? Arguably, the concealment of the contract's terms in code renders it difficult for the plaintiff to interact on an equal footing to the defendant.

The second type of contractual vitiation that may occur widely on the blockchain is misrepresentation. At one stage, a type of fraudulent transaction occurred in abundance in the form of the 'rug-pull', a novel scam facilitated by the blockchain through smart contracts.[431] Although these crypto asset offerings may take the form of a bilateral smart contract if accompanied by a whitepaper or roadmap, they often do not include these natural language indicators of the terms of the agreement.[432] Without an express representation concerning the transaction that precedes the rug-pull, there may be no contract upon which the plaintiff can sue. The reason for this is that no right of the plaintiff has been established in the execution of the smart contract. While on its face a rug-pull transaction is correctively unjust, it may be

[429] Roger Brownsword, 'Smart Contracts: From a Legal Perspective' in Dário Moura Vicente, Diogo Pereira Duarte and Catarina Granadeiro (eds), *FinTech Regulation and the Licensing Principle* (European Banking Institute 2023) 152.
[430] Mark Giancaspro, '"I, Contract": Evaluating the Mistake Doctrine's Application Where Autonomous Smart Contracts Make "Bad" Decisions' (2022) 45 Campbell Law Review 53, 75; Rizos (n 175) 798–799.
[431] There are now fewer rug-pulls than in previous years, but the loss of one's holdings due to them remains significant. See 'Crypto Rug Pulls Have Slowed, but Are Now More Devastating: DappRadar' (*Cointelegraph*, 18 April 2025) <https://cointelegraph.com/news/2025-shaping-up-fewer-but-more-impactful-rugpulls-dapp-radar> accessed 16 July 2025.
[432] See CertiK, 'The Rug Pull Report' (2023) <https://certik.com/resources/blog/the-rug-pull-report> accessed 28 January 2024. In a study conducted by blockchain security auditor CertiK, 87.1% of rug-pull projects did not include a whitepaper, while 77.4% did not have roadmaps.

difficult to reverse a transaction where the 'right' of the plaintiff is found only in the software's code. In other words, when a DASC smart contract to conduct a rug-pull, its purpose is to transfer assets without establishing any right and correlative duty.

In contrast, innocent misrepresentations may take the form of a bilateral smart contract where the defendant innocently states that the smart contract will perform in one way when its code is actually written to perform in a different way. In that context, the plaintiff may have a right to the item promised in the natural language component of the bilateral smart contract, and the defendant a correlative duty to deliver that item by way of the smart contract's code.

5.2 Mistake

Much like traditional contracts, smart contracts are susceptible to mistakes. Arguably, they are more prone to mistakes than fiat contracts when they are reduced to computer code which the parties may not immediately understand. To comprehend their terms, such smart contracts will require time and concentration to decode. As a result, a smart contract may not accurately reflect the parties' mutual will after it has been executed. This is likely to occur where there is a written agreement that includes one set of terms to which the parties have already assented, but the smart contract contains terms that are different or conflict with the written terms. The parties may overlook such a mistake in the code unless the code itself contains an obvious omission which ought to be obvious to one or both parties. Two forms of mistake are recognised under contract law. The first to be addressed in this chapter is common mistake, followed by unilateral mistake.

5.2.1 Common mistake

Common mistake is concerned with contracts that are formed based on a shared incorrect assumption between parties. The courts are reluctant to render contracts void unless they

contain a fundamental mistake.[433] This means that the transaction, if performed, must be radically different from what the parties had intended before a court will hold a contract to be void. In other words, the performance of the contract as intended by the parties must be made impossible. For example, in *Associated Japanese Bank (International) v Credit du Nord SA*, the claimant bank entered a sale and leaseback arrangement with an engineering company for machinery.[434] The defendant bank provided a guarantee for the repayments by the engineering company to the claimants. Unbeknownst to the claimant and defendant, the engineering company did not possess the machinery it intended to sell. Although it was not the *ratio* for the decision, the Court was willing to apply the doctrine of common mistake as the non-existence of the machinery significantly changed the nature of the agreement. As a caveat, the Court also stated that a party cannot rely on a common mistake where he had no reasonable grounds for believing the mistake.[435] Thus, the doctrine of mistake may apply to smart contracts, for example, where one party offers to sell a crypto-asset to the other even though she does not possess such an asset.

The mistake must be fundamental in order to avoid a contract. This is a significant element as it explains why common mistake overrides the existence of a meeting of minds between the parties. There are two situations where a mistake will be considered sufficiently fundamental. First, it must make performance of the contract impossible. A contract may be impossible to perform where its subject matter no longer exists. In *Strickland v Turner*, the parties entered into a contract of annuity in relation to a person who was already dead.[436] They both mistakenly believed that he was still alive, and so the contract was avoided as the subject matter no longer existed. The Court in *Couturier v Hastie* similarly avoided a contract for the delivery of corn

[433] Peel (n 308) 353.
[434] *Associated Japanese Bank (International) v Credit du Nord SA* [1989] 1 WLR 255.
[435] ibid, 268.
[436] *Strickland v Turner* (1852) 7 Ex 208.

from Salonica to England.[437] In that case, the shipmaster sold the corn at Tunis as it began to perish before it could reach the purchaser's location. As such, the subject matter no longer existed. At the time the contract was formed, both the buyer and seller mistakenly believed that the subject matter was still available. Otherwise, *res sua* cases deal with mistakes relating to title where one party transfers ownership of an item to another under the mistaken belief that he owns it. In *Cooper v Phibbs*, one of the parties tried to sell a fishery to the other under the mistaken belief that the purchaser did not already own the fishery. The Court held that this was a sufficiently fundamental mistake so as to render the contract void.[438]

Alternatively, the mistake must make performance 'essentially different' than that which the parties intended.[439] It is not usually sufficient that there is a mistake as to the quality of the subject matter, and only in exceptional cases will the quality of the subject matter be treated as fundamental.[440] Lord Atkin stated in *Bell v Lever Bros* that a non-fundamental mistake may involve the purchase of an art piece under the mistaken belief that it was an original work from a master painter.[441] Unbeknownst to the purchaser, the painting was actually a modern replica. In such a situation, Lord Atkin stated that the purchaser would have no remedy unless the purchaser made a representation as to the authenticity of the artwork.[442] Such a representation could be made on a webpage or whitepaper which provides details regarding the sale of a crypto asset.[443]

---

[437] *Couturier v Hastie* (1856) 5 HL 673.
[438] *Cooper v Phibbs* (1867) UKHL 1.
[439] *Bell v Lever Bros* [1932] AC 161, 218.
[440] *Great Peace Shipping Ltd v Tsavliris (International) Ltd* [2002] EWCA Civ 1407.
[441] *Bell v Lever Bros* [1932] AC 161, 224.
[442] Lord Atkin's conceptualisation of mistake in his hypothetical in *Lever Bros* was confirmed as correct in *Leaf v International Galleries* [1950] 2 KB 86, which is factually similar to the scenario which he outlined: the purchaser bought an artwork which he mistakenly believed was by Constable. The Court held that it was not a fundamental mistake as the purchaser received exactly what he contracted to buy.
[443] Of course, the question may not be whether one is buying an authentic Constable, but whether they are buying an authentic 'Beeple' or 'Bored Ape' NFT. For some of the most expensive NFTs sold, see Stephen Graves, Daniel Phillips and Andrew Hayward, "The 15 Most Expensive NFTs Ever Sold" (*Decrypt*, 21 February 2022) <https://decrypt.co/62898/most-expensive-nfts-ever-sold>.

Where a common mistake has occurred between the parties, the contract may be declared *void ab initio* at common law. The doctrine and the remedy provided by the courts in the case of common mistake recognises that the contract, or smart contract, does not accurately capture the will of the parties. Holding both parties to a contract which neither of them desired contradicts the freedom with which they entered the contract in the first place. Alternatively, a common mistake at equity may attract different outcomes to those at common law, allowing for the contract to be rescinded on terms.[444]

5.2.2 Unilateral mistake

A unilateral mistake occurs when only one party to a contract is mistaken about a material fact concerning the transaction. Cases concerning unilateral mistake often concern mistake as to the identity of a person.[445] In such cases, the consent of the mistaken party is negatived.[446] For example, in *Cundy v Lindsay*, the claimants sent a consignment of handkerchiefs on foot of an order by an individual named Blenkarn.[447] He signed off using the name of an established business, 'Blenkiron & Co'., in order to benefit from its good reputation. He received the goods from the claimants (having not paid for them) and sold them to the defendants. The Court held that the contract was void as the claimants clearly intended to deal with the Blenkiron & Co. company, and not the person named Blenkarn. The problem of mistaken identity might arise in relation to crypto asset transactions as they are addressed to crypto wallet numbers rather than names or email addresses. Instead, crypto wallet numbers consist of a string of alphanumerical

[444] *Associated Japanese Bank v Crédit du Nord* (1989) 1 WLR 255, 266–267: 'Equity will give relief against common mistake in cases where the common law will not, and it provides more flexible remedies including the power to set aside the contract on terms.' (per Steyn J.).
[445] Peel (n 308) 374.
[446] ibid 375.
[447] *Cundy v Lindsay* (1878) 3 App. Cas. 459.

characters. Without a natural language name, it is possible that one party may mistakenly exchange crypto assets with the wrong recipient. If such a mistake occurred in a face-to-face transaction, a Court would hold that the contract is still enforceable.[448]

At equity, the doctrine of unilateral mistake extends beyond the mistaken identity of the contracting parties and may provide relief where one party is mistaken about the contents of the contract and it would be unconscionable for the defendant to benefit from it.[449] In instances of unilateral mistake at equity, the contract will be voidable rather than void. An example of a unilateral mistake as to the terms of the contract is found in *Webster v Cecil*, in which the defendant erroneously offered to sell land for £1,250 instead of £2,250.[450] The defendant instantly informed the plaintiff that he had made a mistake in the offer after the defendant had accepted it. The defendant refused to provide the land to the plaintiff, and as a result, the plaintiff sought to enforce the contract and an order of specific performance from the courts. The courts refused to provide relief because the defendant had immediately acted quickly in informing the plaintiff, and that the courts could not 'compel a person to sell property for much less than its real value, and for £1000 less than he intended'.[451]

To permit the plaintiff to enforce the contract in *Webster* would be unjust because he received notice of the mistake and because of the imbalance in the value. Had both parties carried on without the addressing the error, it would be fair for the courts to enforce the contract. However, a right to contractual performance arises only as far as it accords 'with the mutually consensual exercises of the parties' purposiveness'.[452] By drawing attention to his error, the defendant identified how his initial offer contradicted his purposiveness, therefore calling into question the basis of the plaintiff's performance right. The doctrine of unilateral mistake may therefore

[448] For example, see *Phillips v Brooks Ltd* [1919] 2 KB 243.
[449] Mindy Chen-Wishart, *Contract Law* (5th edn, Oxford University Press 2015) 279.
[450] *Webster v Cecil* (1861) 54 ER 812.
[451] ibid 64.
[452] Weinrib, *Corrective Justice* (n 24) 25.

provide corrective justice by ensuring the rights and duties of the parties manifest the parties' aims for which they contracted.

5.3 Frustration

The doctrine of frustration can be used to discharge contracts where a supervening event occurs which the contract itself does not anticipate. The Irish Supreme Court in *Neville and Sons v Guardian Builders* stated that this supervening event:

> 'must change the nature of the outstanding contractual rights and obligations from what the parties could reasonably have contemplated at the time of the contract's formation that it would be unjust to hold them to its stipulations in the new circumstances'.[453]

In this regard, the foundations of a contractual agreement must be destroyed by the frustrating event.[454] It must be impossible to carry out the terms of the contract or must change the obligation to perform the contract into a significantly different obligation from that originally intended by the parties.[455] A slight adjustment to the parties' obligations caused by the event will not be sufficient to discharge the parties of their duty to perform under the contract. Another essential element of frustration is that the supervening event must not have been contemplated by the parties at the time they formed the contract.[456]

Smart contract transactions may be disrupted by supervening technological events such as cyberattacks, glitches, or mistakes in the computer code. Such events could cost parties significantly if they are expected to undertake the exchange despite a change in circumstances

[453] *Neville and Sons v Guardian Builders* [1995] 1 ILRM 1, 2.
[454] Stephen A Smith, *Contract Theory* (Oxford University Press 2004) 372; *Tamplin SS Co v Anglo-Mexican Petroleum Co* [1916] 2 AC 397, 406.
[455] *Zuphen v Kelly Technical Services* [2000] 5 JIC 2401.
[456] *Davis Contractors Limited v Fareham UDC* [1956] AC 696; *Ringsend Property Ltd v Donatex Ltd & McNamara* [2009] IEHC 568.

that affects the underlying transaction, such as a network outage which renders a crypto asset exchange offline at the time a smart contract was set to be executed.

The courts are reluctant to apply the doctrine of frustration liberally.[457] A contract will not be deemed frustrated simply because it is difficult to perform due to unexpected changes. The case of *Davis Contractors v Fareham UDC* illustrates this point. [458] It involved a building contract in which construction was expected to last eight months at a cost of £94,000. However, the price increased to £115,000 due to problems with labour and building material shortages. The House of Lords held that this contract was not frustrated as there was no fundamental change in the circumstances of the agreement aside from typical commercial risks, and that the loss was not significant enough to amount to frustration. The House of Lords held that 'hardship', 'inconvenience', or 'material loss' alone do not invoke the doctrine of frustration. Rather, the significance of the obligation must have changed so that the contract would be very different from how it was intended by the parties if performed.[459] Therefore, the doctrine will not assist crypto-asset traders affected by the foreseeable commercial risks associated with their trading activities.

There are a number of cases which stress that the frustrating event must not be foreseeable by the parties. First, the circumstances in *Zuphen v Kelly Technical Services* involved the recruitment of the plaintiffs, from South Africa, to work on an Eircom telecoms project.[460] Eircom eventually ceased supplying work to the agency responsible for the plaintiffs' recruitment and they argued that their contracts were frustrated. Murphy J. in the Irish High Court rejected their argument as the agreement between the defendant companies and Eircom stipulated that there was a possibility that work will not be available, and they will only be

[457] McWilliam J. in *McGuill v Aer Lingus* [1983] 10 JIC 0303 stated unambiguously that the alleged frustration "should be strictly scrutinised and the doctrine is not to be applied lightly".
[458] *Davis Contractors Limited v Fareham UDC* [1956] AC 696.
[459] *Davis Contractors Limited v Fareham UDC* [1956] AC 696, 729.
[460] *Zuphen v Kelly Technical Services* [2000] 5 JIC 2401.

allocated work 'as the need arises'. In *McGuill v Aer Lingus,* McWilliam J. stated that the event must be unexpected by all parties, and that a contract is not frustrated where one party anticipated or should have anticipated the event.[461] Where an event is or should be anticipated by the parties, he stated that they should provide for this in the contract.[462] However, this position contrasts with that in *Ocean Tramp Tankers Corp v V/O Sovfracht, The Eugenia,* where Lord Denning M.R. stated that the idea that frustration is only applicable in 'uncontemplated' events is untrue. He stated that 'the only thing that is essential is that the parties should have made no provision for [the event] in their contract'.[463]

The parties will often determine how foreseeable events should be handled expressly in the contract. Yet, foreseeability alone will not prevent the courts from finding that a contract has been frustrated. This position was adopted in *Neville and Sons v Guardian Builders*, in which both parties knew they required permission from the County Council in order to perform a building contract. Despite the (foreseeable) risk that the Council could decline to give permission for construction, the High Court was satisfied the doctrine of frustration was applicable.[464] Although these are contradictory positions provided by different judgments, there is more emphasis by the courts on whether it would be unjust to hold parties to the terms of a contract where a supervening event has caused a significant change in circumstances that substantially affect the contract if it was performed.[465] Therefore, the doctrine may be used by the courts where the performance of the smart contract significantly varies beyond what the parties agreed. For example, if a crypto-asset exchange used by the parties suffers a cyber-

[461] *McGuill v Aer Lingus* [1983] 10 JIC 0303.
[462] ibid.
[463] *Ocean Tramp Tankers Corp v V/O Sovfracht, The Eugenia [1964] 2 QB 226, 239.*
[464] *Neville and Sons v Guardian Builders* [1990] ILRM 601, 615. The Supreme Court later reversed the decision in this case on other grounds, but also seemed to accept that frustration may apply in relation to foreseeable events.
[465] *Kenneth Treacy v Lee James Menswear Ltd and James O'Regan* [2022] IEHC 600, para 11; *Redfern Limited v Larry O'Mahony and Thomas McFeely* [2010] IEHC 253.

attack affecting the output of the smart contracts, they may be frustrated if the attack was unforeseeable.

The doctrine of frustration may reflect the principles of corrective justice.[466] The correlativity of contracting involves one party's right which mirrors the other party's duty. When a frustrating event occurs, the correlative interaction collapses. If the contract was upheld, the plaintiff would have a right to performance while the defendant would be unable to perform his duty. The doctrine itself operates correlatively as it discharges both sides from their future obligations. In doing so, the doctrine disables future wrongs (potentially subject to a breach of contract claim) by preventing the further transfer of benefits from the point of the supervening act. The difference between frustration and breach of contract is that the former does not involve damages because liability would imply that one party acted wrongfully. The doctrine of frustration also respects the parties' interaction as free beings as it must only be used as a last resort.[467] It favours the contract's validity by upholding the parties' choices where possible.[468]

5.4 Misrepresentation

Misrepresentation occurs when an individual is enticed to enter a contract on the basis of a misleading statement.[469] The doctrine of misrepresentation is relevant in the analysis of contract law's response to crypto-asset transactions as smart contracts can be used to facilitate exchanges made based on misleading statements. The three elements required to prove

[466] Although this idea is doubted by some. See Guanghua Yu, 'The Theoretical Foundation of the English Doctrine of Frustration: Efficiency or Justice?' (2019) 7 City University of Hong Kong Law Review 47, 56–57.
[467] *The Super Servant Two* [1990] 1 Lloyd's Rep 1, 8: 'Since the effect of frustration is to kill the contract and discharge the parties from further liability under it, the doctrine is not to be lightly invoked, must be kept within very narrow limits and ought not to be extended.' (per Bingham L.J.).
[468] Andrew Phang, 'Frustration in English Law - A Reappraisal' (1992) 21 Anglo-American Law Review 278, 295.
[469] Peel (n 308) 410.

misrepresentation were set out in the Irish High Court by McCracken J. in *Colthurst v La Touche Colthurst*.[470] He stated that a misrepresentation consists of an untrue factual statement, which enticed the plaintiff to enter into the contract. First, a representation must be made. The representation need not be in oral or written form and may be made in some other way.[471] In addition, silence may amount to a representation. For example, in *Gill v McDowell*, the fact that the owner of a cow did not inform the market that the animal he was selling was a hermaphrodite was held by Lord O'Brien C.J. to be a misrepresentation.[472] Thus, the courts may assess a party's attempt to conceal the poor quality of a crypto-asset through the doctrine of misrepresentation.[473]

In order to be a misrepresentation, it is essential that the statement is untrue. The courts will not punish minor inaccuracies in a statement, but half-truths may be considered as false representations. Additionally, statements that were once true but subsequently become untrue may be construed as misrepresentations, and the person making the statement ought to inform the recipient of the circumstantial changes.[474] A similar rule applies where the person making the statement believes it to be true but is incorrect in this belief. Thus, if he discovers that his statement is untrue during negotiations, he has an obligation to correct his mistake.[475]

The statement must be a representation of fact. However, sales puffs, opinions, and statements of intention do not usually amount to statements of fact. This point is particularly relevant to misrepresentation and how it applies to crypto asset transactions. Many alleged

[470] *Colthurst v La Touche Colthurst* (Unreported, High Court, 9 February 2000).
[471] In *Ridge v Crowley* (1958) 172 EG 637, the defendant concealed defects in a house's foundations. His conduct was held to constitute a representation.
[472] *Gill v McDowell* [1903] 2 IR 463.
[473] A poor quality crypto asset may be one that does not have any serious use case. See Brian Quarmby, '"Most of Crypto Is Still Junk" and Lacks Use Case — JPMorgan Blockchain Head' *CoinTelegraph* (30 August 2022) <https://cointelegraph.com/news/most-of-crypto-is-still-junk-and-lacks-use-case-jpmorgan-blockchain-head> accessed 28 July 2023.
[474] *With v O'Flanagan* [1936] Ch 575. This case revolved around the sale of a medical practice. The seller stated that it was worth £22,000, but its value subsequently declined to £5 as he fell ill.
[475] *Davies v London & Provincial Marine Ins Co* (1878) 8 Ch D 469.

misrepresentations may be based on the enticements contained in marketing statements that are used to advertise new cryptocurrencies or NFTs to investors. Therefore, it is important to understand the difference between an actionable misrepresentation, and statements which the courts will disregard as mere statements of intent, opinion, or sales puff.

To begin, a sales puff is an exaggerated statement about the product for sale. Sales puffs do not amount to actionable misrepresentations as a reasonable person would not attach much significance to them. The distinction appears to be between statements that are detailed and those which provide vague descriptions of the subject matter.[476] Therefore, a statement which promoted piece of land as 'fertile and improvable' did not amount to a misrepresentation in *Dimmock v Hallett* because it lacked specificity.[477] However, a statement which provides precise detail regarding the transaction would not be considered as a mere puff. Additionally, the party's conduct may indicate that the statement is not mere puff.[478] This rule may be useful to distinguish between attempts to promote a genuine crypto asset against efforts by parties to mislead a buyer into purchasing a worthless asset.

Similarly, statements of intention do not typically constitute misrepresentation. Once again, there is a distinction between statements of intention which were honestly made and those which were not. Essentially, this means that a statement is not a misrepresentation if the person who made the statement honestly believed it to be true. In *The Seaflower*, a ship's owners said they would acquire the approval of an oil company within a certain period of time.[479] They ultimately did not receive approval, yet the Court held that this was not a misrepresentation as the ship's owners had honestly intended to acquire it. However, where an individual makes a

[476] Clark (n 182) [11-12].
[477] *Dimmock v Hallett* [1866] LR 2 Ch App 21.
[478] For example, in the classic case of *Carlill v Carbolic Smoke Ball Co* [1893] 1 QB 256, 261, Lindley L.J. held that a statement about the efficacy of the carbolic smoke ball in curing influenza was not mere puff as the defendants entered £1000 into the bank to indicate their sincerity.
[479] *The Seaflower* [2000] 2 All ER (Comm) 169.

statement of intent which they do not genuinely hold, then that statement may be held as one of fact. For instance, in *Edgington v Fitzmaurice*, the directors of a company sought submissions for debentures by issuing a prospectus. Within the prospectus, they said they intended that the money would be used to upgrade the company's buildings and to purchase horses for transport. However, they actually intended to pay off liabilities using the acquired money. Bowen L.J. stated that, although it is not always possible to determine a person's state of mind, it may be 'as much a fact as anything else' if it can be ascertained.[480] He further stated that 'a misrepresentation as to the state of a man's mind is, therefore, a misstatement of fact'.[481] He arrived at this conclusion because the defendants had suffered financial difficulties and could not afford to pay off a mortgage that they had taken out.[482]

Statements of opinion differ from statements of intention as the courts may consider whether the recipient reasonably considered the statement of opinion to be one of fact.[483] Thus in *Bissett v Wilkinson*, the Court held that a statement claiming that a field could facilitate 2,000 sheep was not a misrepresentation.[484] This was due to the fact that the seller of the land indicated this was merely his opinion, and that the buyer knew he had no special knowledge about land for agricultural use. In contrast, *Esso Petroleum v Mardon* shows that if a person makes a statement using care and skill to calculate figures, the Court will deem his statement as a misrepresentation.[485] In that case, an oil company informed a garage operator that a specific location would result in a specific number of sales. Had the garage operator merely made an estimate in its statement, the outcome would have been different. Therefore, a statement

[480] *Edgington v Fitzmaurice* (1885) 8 App Cas 467, 483.
[481] ibid.
[482] ibid, 480.
[483] Clark (n 182) [11-05].
[484] *Bissett v Wilkinson* [1927] AC 177.
[485] *Esso Petroleum v Mardon* [1976] QB 801.

supported by the party's expertise and is made with a degree of certainty may be more readily held as a misrepresentation.

The final element of the test for misrepresentation requires that the statement must have induced the other party to rely on it. In *Smith v Chadwick*, the purchaser claimed that there was a misrepresentation in a contract for the sale of shares.[486] However, the Court dismissed his claim as the representation did not actually impact his decision to purchase the shares and he was going to buy them regardless. More recently in *Intrum Justitia v Legal and Trade Financial Services Ltd*,[487] the Irish High Court rejected a claim of misrepresentation where the plaintiff sought to purchase the shares of a company. The defendant stated that their company had 'no skeletons in the cupboard'.[488] As the plaintiff company had carried out its own examination as to whether it should purchase the shares, O'Sullivan J. held that the representation made by the defendant had no bearing on the plaintiff's decision to buy shares.[489]

Whether fraudulent, innocent or negligent, the doctrine of misrepresentation endeavours to provide corrective justice. By misrepresenting the content of a contract, the representor takes away the representee's ability to decide the ends which he rationally seeks. He expects, and acquires a right to, one outcome yet ultimately receives something else than what the representor had a duty to provide. In *Esso Petroluem*, the representee was entitled to tenancy of a petrol station that was capable of selling 200,000 gallons of fuel which instead lost money. Correlatively, the representor had a duty 'to use reasonable care' to ensure the representation is accurate and the information provided is dependable.[490] For negligent misrepresentation, damages in lieu of rescission are assessed according to the cost of correcting the defect. Where the misrepresentation is negligent or fraudulent, damages are recoverable in tort rather than

[486] *Smith v Chadwick* (1884) 9 App Cas 187.
[487] *Intrum Justitia v Legal and Trade Financial Services Ltd* [2009] 4 IR 417.
[488] ibid, para 27.
[489] ibid, para 30.
[490] *Esso Petroleum v Mardon* (n 458).

contract. The objective of damages is to put the plaintiff in a position as though the wrong had not occurred.[491] In other words, the wrongful gains and losses of the parties are eliminated by way of damages by removing the defendant's gain and returning it to the plaintiff, thereby restoring the equality between the parties.[492]

In summary, there are many instances where legal doctrines relating to the vitiation of contracts may be applied specifically to smart contracts. The following section examines how suitably smart contracts map to these doctrines, and whether corrective justice may be obtained in smart contract transactions.

5.5 The vitiation of smart contracts

The following section discusses smart contracts as they might be used in two different contexts. First, the 'bilateral smart contract' involves a transaction which is initiated off-chain. The offer may be presented in-person on paper, or contained in a digital document. What distinguishes it from other types of smart contracting is that it involves a natural language agreement which states the terms of the contract clearly in a way that can be understood by human parties. The blockchain in this context is used to ensure performance and record the transferal of rights that takes place according to the terms of the agreement.[493] The second type of smart contract considered, the DASC, is used in Web 3.0 and crypto asset transactions such as for the investment in initial coin offerings, and the exchange of cryptocurrencies and NFTs. Unlike in bilateral smart contracts, parties who use DASCs interact without any previous communication and have no way of truly knowing the identity of the individual on the other side of the transaction. They instead enter into transactions based on minimal information. Accordingly, it

[491] McKendrick, *Contract Law* (n 166) 238.
[492] Ernest J Weinrib, 'The Gains and Losses of Corrective Justice' (1994) 44 Duke Law Journal 277, 280.
[493] Filatova (n 19) 228.

may be unclear as to whether the establish the correlative right and duty used in corrective justice to determine whether an actionable injustice occurred.

This distinction, as I will argue over the course of this chapter, is an important one because contract law may be more familiar with the structure of bilateral smart contracts. Under these contract types, more background context to the transaction is available to the courts which they may examine to determine whether the consent of either party has been vitiated. Given that DASCs lack such background context as they tend to be 'once off' in nature, it may be difficult to determine the terms to which the parties actually agreed. Furthermore, the lack of any plain language agreement renders it difficult to determine whether the smart contract has been vitiated because the code will have performed as it was written. Although it may not reflect the parties' intentions, the performance of the isolated smart contract may be upheld because the code performed as it was instructed to by its writer. Without additional context, it will be difficult to discern what the parties objectively intended.

This section begins by addressing how bilateral smart contracts may be vitiated, focusing on the how code may deviate from the parties' initial understanding of the agreement. It then turns to the more problematic decentralised algorithmic smart contract.

5.6 Smart contracting mistakes

5.6.1 Unravelling Mistake in BSCs

Mistakes may occur in a bilateral smart contract as the smart contract may not accurately reflect the terms of the parties' agreement situated off-chain. For example, a smart contract drafter may mistakenly write a value into the programme's code that does not correspond with the parties' pre-existing agreement. The mistake may be attributed to basic human error as the drafter may be pre-occupied with writing the code and may enter the wrong value as a result. From a corrective justice perspective, the error results in performance that does not reflect the

parties' agreed normative relationship. As such, corrective justice requires that equilibrium is restored by undoing the transfer of the benefit or burden resulting from the mistake.

For instance, the parties in *Great Peace Shipping Ltd v Tsavliris (International) Ltd* may have used a smart contract had the technology been available at the time.[494] That case involved the chartering of a vessel for a minimum of five days to undertake the rescue of another vessel in distress. When the parties agreed to charter the vessel, they both laboured under the incorrect belief that the Great Peace was 35 miles away, rather than 410 miles. The UK Court of Appeal held that contract was not void because the *Great Peace* would have arrived at the site of the stricken vessel in sufficient time, thus the owners of the vessel were entitled to payment.[495] The contract was not held void as performance of it was still possible and would not have been essentially different from the performance anticipated by the parties. The outcome exemplifies corrective justice by upholding the parties' contract because it did not differ from the parties' self-determined purposiveness as the rescue vessel would reach the distressed vessel within an appropriate timeframe. It would therefore be unfair to hold the contract voidable because the mistake was not so serious so as to render performance significantly different from the performance that the plaintiff could expect under the right obtained under the contract.

However, had the circumstances been different (i.e. had the rescue vessel been incapable of reaching the stricken vessel in sufficient time), corrective justice would require that the contract be unwound. And had a smart contract governed the parties' arrangement (e.g. payment may be executed automatically when the vessel arrived at coordinates stipulated in the contract's code), the code may have ensured performance notwithstanding the background norm of mistake. This is concerning from a corrective justice perspective as the loss would be suffered by the plaintiff and the other party would have obtained a gain. Consequently, corrective justice

[494] *Great Peace Shipping Ltd v Tsavliris (International) Ltd* [2003] QB 679.
[495] *Great Peace Shipping Ltd v Tsavliris (International) Ltd* [2003] QB 679.

would require that the transaction be unwound to restore parties to their original, pre-contractual position.

In a bilateral smart contract, it is at least possible to identify such mistakes so as to bring the whole agreement in line with the parties' self-determined purposes which they had manifested by initially entering the contract. A further example may be found in *Associated Japanese Bank (International) Ltd v Credit du Nord*.[496] In that case, the plaintiff and defendant mistakenly believed the representations made by a third-party as to the existence of precision engineering machines. The plaintiff bank provided financing for the machinery on the basis that the defendant bank provided a guarantee for it. When it was revealed that the third-party had lied about the existence of the machines, the plaintiff sought to rely on the defendant's guarantee. On this basis, the Court held that the contract was void because the existence of the machinery was fundamental to the existence of the contract. Unlike in *Great Peace Shipping*, the plaintiff had suffered a normative loss in providing financing to the defendant on foot of the third party's lies. Although the contract embodied the parties' purposiveness, once it was apparent that the machinery did not exist, their right and duty is extinguished because performance is not possible.

If this agreement was executed using a smart contract, the code could be written in a way that the loan will be released once the guarantee had been submitted to a destination stipulated in the smart contract (e.g. a particular email address with a particular subject). However, a smart contract may not have knowledge of the non-existence of physical objects such as the machinery in the case. Nonetheless, the courts may look to the parties' plain language agreement including the guarantee and any statements made by the third party. This way, they

[496] *Associated Japanese Bank v Crédit du Nord* (n 417).

can determine whether the defendant is still in a position to fulfil its duty of performance. If the answer is negative, the whole bilateral smart contract arrangement may be unwound.

5.6.2 Mistake in DASCs

The potential for mistake poses a problem for DASCs. Unlike bilateral smart contracts wherein the parties know each other, these smart contracts are characterised by their anonymity coupled with their immutability. Moreover, their content is contained entirely within their code. As previously discussed, both parties can coordinate to correct any mistakes that occur in a bilateral smart contract transaction by creating a new smart contract. However, with added anonymity, the identity of a party that has benefitted from a mistake may remain concealed.[497]

In the instance of a mistake, corrective justice requires that the mistaken party should not be held to the terms of the agreement so long as the offeree knew the offeror had erred in her offer. The reason is that the offeror has not in fact agreed to the arrangement to which she had assented because she believed she had assented to something else.[498] The consequent agreement is not a result of the offeror's will and does not bring about her purposes.[499] As such, the offeror should be excused from performance of the contract, otherwise the resulting transaction would be correctively unjust.

However, corrective justice may not be achieved in a smart contract transaction involving a mistake. This is the result of the courts trying to strike a balance between upholding parties' bargains (mediated by technology) and voiding the contract because the parties are significantly at cross-purposes that an agreement is not concluded.[500]

---

[497] Giancaspro, 'Is a "Smart Contract" Really a Smart Idea?' (n 216) 827.
[498] Alan Brudner, 'Hegel and the Crisis of Private Law' in Drucilla Cornell, Michel Rosenfeld and David Gray Carlson (eds), *Hegel and Legal Theory* (Routledge 1991) 168.
[499] ibid.
[500] Peel (n 308) 374.

Quoine Pte Ltd v B2C2 Ltd illustrates the dilemma between reversing or upholding a smart contract concluded because of a mistake.[501] The purported mistake in that case was found in a smart contract that was used to trade Bitcoin for Ether cryptocurrency. Due to a technical oversight by Quoine, a number of trades executed at approximately 250 times over the market value at the time.[502] The Singaporean Court of Appeal held there was no mistake at common law or in equity, on the basis that the parties used algorithmic software to execute the trades.[503] As such, the parties did not know they were going to enter into the trades, or the terms underlying the trades.[504] Had there been a natural language document that outlined the terms of the smart contract, the Court may have found that there was a mistake that could be relied upon to render the smart contract void. However, the Court was satisfied in this case that the pre-programmed transactions were executed exactly as they were coded so there could not have been a mistake.[505]

The transactions in *Quoine* may be correctively unjust because the offeror had agreed to terms other than those ultimately concluded within the smart contract. The resulting agreement did not bring about Quoine's purposes – of which can be approximated by looking at how margin calls on the platform usually operate.[506] Prior to the breakdown of Quoine's system, the value of their trades ranged from 0.039 to 0.045 BTC/ETH.[507] This would suggest that the disputed trades of 10 whole Bitcoins for 1 Ether were mistakenly executed.

Before its analysis of unilateral mistake, the Court stated that it would apply the doctrine 'subject to incremental adjustments being made in order to suit the particular context' of

[501] *Quoine Pte Ltd v B2C2 Ltd* (n 216).
[502] ibid, para 152.
[503] ibid, para 183.
[504] ibid, para 97.
[505] ibid, para 114.
[506] i.e. before Quoine's software ceased functioning.
[507] The process is explained by Simon Thorley I.J. in the High Court judgment. See *B2C2 Ltd v Quoine Pte Ltd* (n 127) [78].

deterministic smart contracts.[508] Moreover, it stated that legislative intervention *may* be required to govern algorithmic contracts, but found that the existing law could be 'meaningfully adapted' to the dispute at hand.[509] A central authority referred to by the Court is the Singapore High Court case *Chwee Kin Keong v Digilandmall.com Pte Ltd* which resembles English law on the matter of unilateral mistake as the parties' subjective intentions are disregarded.[510] The offeree must have actual knowledge of the offeror's mistake. If the offeree has such knowledge, then he cannot claim that there was a meeting of minds.[511] This is the rationale of the doctrine of unilateral mistake. The parties are not linked doctrinally through offer and acceptance because the offer contains a flaw and therefore a juridically intelligible relationship is not formed.[512] Yet, the Court in *Quoine* was satisfied that a contract was formed notwithstanding Quoine's error.

The reason the Court found against Quoine was that the doctrine of unilateral mistake is concerned with a mistake as to the fundamental terms of the contract (at common law), and whether the non-mistaken party knew or ought to have known about the mistake and took advantage of it. The Court found that the parties were determined to use algorithms to transact which prevented them from knowing when a contract would be formed or what would be its fundamental terms, and therefore it was unwilling to intervene in the transaction after it was executed.[513] This signifies that parties may be *ad idem* as to the use of algorithms to contract, but that it is difficult to know that the resulting contract will serve the purposes of one or both parties.

[508] *Quoine Pte Ltd v B2C2 Ltd* (n 216) [79].
[509] ibid.
[510] *Chwee Kin Keong v Digilandmall.com Pte Ltd* (2005) 1 SLR(R) 502; Kelvin FK Low and Eliza Mik, 'Lost in Transmission: Unilateral Mistakes in Automated Contracts' (3 May 2020) 2 <https://papers.ssrn.com/abstract=3591657> accessed 22 March 2024.
[511] *Quoine Pte Ltd v B2C2 Ltd* (n 216) [81].
[512] Weinrib, *Idea* (n 14) 28–29.
[513] *Quoine Pte Ltd v B2C2 Ltd* (n 216) [104].

At common law, the non-mistaken party must have actual knowledge as to the mistake, while at equity he must have constructive knowledge. For its common law analysis, the Court adopted the test as set out in *Digilandmall.com* in which knowledge is ascertained according to the 'experiences and idiosyncrasies of the person and what a reasonable person would have known in a similar situation'.[514] However, the non-mistaken party may not know the experiences and characteristics of a party whose transactions are often executed using a DASC. Therefore, the non-mistaken party's knowledge may be constructive at best.

Unlike the requirement of actual knowledge, a party has constructive knowledge of the error if the mistake would have been identified by a reasonable person in the position of the non-mistaken party.[515] For instance, if the non-mistaken party 'shuts its eyes to the obvious, it is neither honest nor reasonable' and it can therefore be held as knowledgeable of the error.[516] However, the Court in *Quoine* found no constructive knowledge on the part of B2C2. The reason was that B2C2's programmer, a Mr Boonen, lacked knowledge of the error between the points of writing the algorithm and the formation of the contract. Although he suspected there was a mistake in the transaction *after* it had executed, the Court found that this was irrelevant because it occurred outside of the 'relevant time frame' for assessment of the mistake.[517] He made his suspicions known to Quoine in an email with the subject line 'Major Quoine database breakdown, please call us urgently'. Although Quoine argued this email was definitive proof that B2C2 knew of the mistake, its knowledge of the mistake was too late to render the contract voidable.

Ultimately, the Court in *Quoine* did not rectify the wrong inflicted by one party on the other, as corrective justice demands.[518] To be sure that an injustice occurred, Quoine must have

[514] *Chwee Kin Keong v Digilandmall.com Pte Ltd* (n 483) [41].
[515] *Quoine Pte Ltd v B2C2 Ltd* (n 216) [108].
[516] Ter Kah Leng, 'Who Bears the Risk of Mistake?' (2004) 20 Computer Law & Security Report 396, 397.
[517] *Quoine Pte Ltd v B2C2 Ltd* (n 216) [125].
[518] Weinrib, 'Corrective Justice in a Nutshell' (n 13) 349.

incurred a normative loss and B2C2 must have obtained a normative gain. The correlative gain and loss involved are the 'quantified manifestations' of B2C2's wrongdoing.[519] Where these elements are present, corrective justice requires that the effect of the defendant's action is undone.[520]

A party obtains a normative gain where it has more than to what it is entitled, and a normative loss when a party has less than it ought to have. If these conditions are met, the defendant's holdings may be decreased. Effectively, the Court found that B2C2 made a normative loss when Quoine reversed the transactions, thereby (in the Court's view) illegitimately decreasing B2C2's resources. However, it may be that Quoine the suffered the normative loss and therefore was correct in its argument that the contract was voidable. Mance I.J. addressed the matter of justice in his dissenting judgment, in which he stated that

> 'The law must be adapted to the new world of algorithmic programmes and artificial intelligence, in a way which gives rise to the results that reason and justice would lead one to expect'.[521]

Quoine's loss was more than just a factual loss. It was a normative loss brought about mistakenly by the parties' communicating algorithms. Quoine (metaphorically) did not just mistakenly pave B2C2's driveway without B2C2's knowledge.[522] Had B2C2 not subsequently detected the error, there would only have been a factual loss and no normative loss for which Quoine could claim. However, the transactions can only be explained as the consequence of serious error which B2C2 'observed concurrently or considered early next morning'.[523] The

[519] Weinrib, 'The Gains and Losses of Corrective Justice' (n 492) 288.
[520] Or in this case, the respondent's actions. ibid 288.
[521] *Quoine Pte Ltd v B2C2 Ltd* (n 216).
[522] The metaphor used here turns back to the hypothetical used by Weinrib to describe instances where a factual gain arises, but no normative gain. See Section 2.4.1.
[523] *Quoine Pte Ltd v B2C2 Ltd* (n 216) [201] (per Mance I.J.).

market conditions for which B2C2 had programmed its algorithm were 'unfathomable' – a fact which B2C2 ought to have known because it was well informed about market conditions.

Notwithstanding B2C2's evident knowledge of the mistake, unilateral mistake in equity requires unconscionability by the non-mistaken party to render the contract voidable. If B2C2 did not act unconscionably, there is no wrongdoing on their part, and they have made no normative gain. Although the majority found there was no unconscionable conduct by B2C2, such unconscionability may be constituted by B2C2's retention of the benefit it received from the transaction.[524] Again, had not B2C2 noticed the mistaken transaction, then Quoine may have no grounds for complaint. However, the reality of the situation was that B2C2 had knowledge of the mistake and was reluctant to relinquish the benefit it obtained as a consequence of it.

Yet, the difficulty is that the law and equity do not recognise the type of knowledge that B2C2 had. Both constructive and actual knowledge requires 'human involvement *during* the relevant transaction'.[525] B2C2's knowledge of the error came only after the transaction was executed. To rectify the imbalance in the parties' holdings, the law requires a principle for scenarios where a mistake would have been noticed had a party been actively involved in the interaction (rather than an algorithm), or once the the mistake is identified post-transaction.[526] In sum, the outcome of *Quoine* does not conform to corrective justice, and algorithmic trading (via DASCs) requires the intervention of unilateral mistake in equity to achieve anything close to it.[527]

[524] ibid 205.
[525] ibid (emphasis added).
[526] Mance I.J. effectively carves out this principle, and bases his conclusion on it. See ibid 206 ['If it is immediately obvious that a mistaken transfer has occurred, a failure to do the honourable thing and return the benefit can be as unconscionable as the conduct of someone who plays some positive part in bringing the transaction about'].
[527] Alexander Loke, 'Mistakes in Algorithmic Trading of Cryptocurrencies' (2020) 83 The Modern Law Review 1343, 1353.

Quoine is just one example of a mistake in a smart contract with significant financial consequences for the mistaken party. Smart contracts will execute regardless of errors included in their code.[528] If the courts are unwilling to hold a smart contract as voidable for mistake, erroneous transactions for significant sums of money will be upheld or enforceable by the non-mistaken party.

5.6.3 DAO mistake

As I have argued in previous sections, smart contracts between two parties are susceptible to mistakes because errors in computer programmes are inevitable.[529] DAOs are formed using a multilateral nexus of smart contracts used to manage the virtual organisation's operations as well as its participants. The end-objective of the typical DAO is to be run almost entirely by the algorithms coded into their architecture. Due to the increased number of smart contracts and the multiplicity of potential parties involved in the various transactions that take place within a DAO, the likelihood of mistake is increased.

For example, a DAO may be formed to manage investment funds pooled together by its investors, the purpose of which is to pursue collective investment opportunities. When participants invest in the DAO, they receive a share of the DAO's tokens proportionate to their investment which provides them with the right to vote on potential investments and treasury spending. A mistake may arise where the DAO's participants vote to invest 1 Bitcoin in a certain blockchain project, but the smart contract ultimately deployed between the DAO and the beneficiary of the investment contains a typo in its code, a consequence of which means

[528] Mik, 'Smart Contracts' (n 2) 104.
[529] Eliza Mik, 'Much Ado about Artificial Intelligence or: The Automation of Contract Formation' (2022) 30 International Journal of Law and Information Technology 484, 502.

that the beneficiary will receive 10 Bitcoin instead. The effect of the transaction almost exhausts the DAO's fund pool.

If the error was contained in a straightforward smart contract between two parties, the mistaken party may plead unilateral mistake. In the DAO scenario however, the consequence of the mistake is felt more widely by the DAO's membership rather than being limited to a bipolar contractual relationship.[530] The question then is *who is entitled to claim that the smart contract should be voided for mistake*? And similarly to DASCs, is there a mistake if the smart contract is constituted by code?

The mistake in this instance may be characterised as a unilateral mistake. A mutual mistake arises where the parties are at cross-purposes to one another and do not share the same mistake. The recipient of the investment analysed the code and believed it was entitled to the 10 Bitcoin. Some of the DAO's members also believed that the code correctly reflected the value of the project's entitlement. However, the remaining DAO members thought that the maximum investment for the particular project was 1 Bitcoin.

There is a common mistake between the recipient project and the first half of the DAO's membership in believing that the project was entitled to receive 10 Bitcoin. A common mistake arises where the parties are labouring under the same mistake as to an important fact relating to the contract. If the courts find that the mistake was fundamental, the consent of the parties may be nullified. However, there is a unilateral mistake between the recipient project and the remaining DAO participants.

[530] The investment is not a gift as the recipient would undertake to use the funds in a particular way that aligns with the DAO's values.

To reestablish the equality between the parties, the courts would have to determine whether the norm permits the removal of the recipient's gain and returning it to the DAO's fund.[531] Whose intention, and therefore which mistake, will be the core of the court's analysis?

If we accept the common mistake analysis to be correct, then the DAO as a collective will be unable to correct their losses. The reason for this is that parties who enter contracts 'with minimal knowledge of the facts to which the mistake relates but is content that it is a good speculative risk' may not be entitled to relief.[532] The DAO's participants may have only a minimal knowledge of the facts because the transaction was executed entirely by the smart contract which was authorised through the voting process. By voting to execute the smart contract, they were potentially engaging in a speculative risk that does not necessitate relief. The reason is that there was no normative gain by the project and no normative loss by the DAO's participants under the common mistake doctrine. On its face, it appeared that the parties' purpose was to exchange 10 Bitcoin. However, the consequence of their decision is felt also by their peers who may have lost a significant sum of their investment because of the executed smart contract.

The other portion of the DAO's members may claim that they operated under a unilateral mistake akin to that made by the defendant in *Webster v Cecil*.[533] The defendant accidentally offered to sell a piece of land for £1250, having previously offered to sell the land for £2000, an offer which the plaintiff accepted but the defendant refused to perform. The plaintiff was aware that the defendant had erred in making the offer, therefore the Court refused to grant an order of specific performance. However, in relation to the DAO, there was no previous offer to which its members could refer to argue that there had been a mistake. And similarly to *B2C2 v*

[531] Weinrib, 'Corrective Justice in a Nutshell' (n 13).
[532] *Associated Japanese Bank v Crédit du Nord* (n 417).
[533] *Webster v Cecil* (n 423).

Quoine, the members may struggle to show that the DAO had actual knowledge of the mistake.[534]

However, there may be a normative basis for the DAO's membership to recover in this instance. The project that received the funding made a wrongful gain at the expense of the members, requiring the restoration of the equality between parties. Although the smart contract established a right between the parties entitling the project to performance in the form of an exchange of 10 Bitcoins, the right was created on a flawed basis. The reason is that the majority of the membership voted to provide 1 Bitcoin, therefore the transaction was not in line with the mutual consent of the parties.[535] As such, the DAO's membership should be under no duty to provide the 10 Bitcoin. The project ought reasonably to have been aware that the DAO's participants did not intend to provide it with 10 Bitcoin because this amount far exceeds the project's needs.[536] Although the parties will typically be held to the contracts they enter notwithstanding their mistake (for the sake of commercial certainty), the exception to this rule lies where the offeree knows the offeror did not intend the words used to express the offer.[537] However, the exception in *Shogun Finance* relates to how two parties will understand natural words used and the effect given to them. Code may only have one meaning.[538] It is evident therefore that the law may not permit corrective justice in the context of DAO transactions.

[534] *B2C2 Ltd v Quoine Pte Ltd* (n 127) [188].
[535] Weinrib, 'Corrective Justice in a Nutshell' (n 13) 354.
[536] 10 Bitcoin is worth approximately €920,000 at the time of writing.
[537] *Shogun Finance v Hudson* [2004] 1 AC 919, 964.
[538] Cannarsa (n 229) 106.

5.7 Misrepresentations in smart contracts

5.7.1 Bilateral smart contract misrepresentation

Smart contract transactions may contain misrepresentations; either innocent, negligent or fraudulent.[539] This section focuses on how these misrepresentations arise in bilateral smart contracts where the transaction is between two identifiable parties who execute the exchange using code. In such a transaction, a misrepresentation is likely to occur where one of the parties makes a pre-contractual promise which is not subsequently reflected in the code of the smart contract. Thus, parties have a duty to act carefully during the negotiation process and must ensure that they can facilitate via smart contract what they promised to the other party.[540] Under section 45(1) of the Sale of Goods Act 1980, a representor may be liable for non-fraudulent misrepresentations unless he can demonstrate that he reasonably believed the statement was true at the time when he made it.[541]

One such claim of innocent misrepresentation is found in *Leaf v International Galleries* in which Leaf purchased – what he believed to be – an authentic John Constable painting.[542] His legitimate belief derived from a representation made by International Galleries as to the painting's authenticity. It was only when he tried to sell the painting five years later that Christie's auction house informed him that it was not in fact a Constable original. International Galleries maintained that the painting was not a forgery. The Court found that International Galleries had made an innocent misrepresentation. The outcome of the case may be explained in terms of corrective justice. Through the interaction, Leaf had obtained a right to performance in which he would obtain a genuine Constable painting. Through the interaction, International

[539] Fraudulent misrepresentation is discussed in the next section on DASCs in relation to a particular type of crypto-asset related fraud viz 'rug-pull' scams.
[540] Collins (n 167) 183.
[541] Sale of Goods Act 1980, s 45(1).
[542] *Leaf v International Galleries* (1950) 2 KB 86.

Galleries obtained a duty to provide no other painting than that which they had represented to him. Because International Galleries provided a different painting, Leaf suffered a normative loss that the courts consequently held *may* be rescinded, while International Galleries obtained a normative gain based on the misrepresentation.[543]

In a bilateral smart contract context, the plaintiff may acquire a right to performance to which the defendant has a correlative duty to provide him with digital artwork in the form of an NFT.[544] There is scope for potential innocent misrepresentations in such transactions except here, the art may not be Constable or Monet paintings, but rather a collective of artists now able to easily monetise and transfer their digital artwork using the blockchain. These digital works may not be as desirable as the classical works that came before, however buyers may still be willing to pay a significant sum of money for them. This is illustrated by the sale of 'Everydays: The First 5000 Days' by Mike Winkelmann (artist name 'Beeple') for $69 million in 2021.[545] This work was a collage of five thousand individual pieces of digital artwork created over the course of five thousand days. Winkelmann has established himself as one of the leading authors of digital art.

What if a buyer purchases a piece of digital work under the reasonable belief it is an 'authentic' Winkelmann work? His belief that it is an original derives from the fact that the seller made a representation to that effect. However, the seller did so innocently as the previous owner of the work also told her that the work was an original. The issue here is that digital artwork is easier to manipulate or clone than physical paintings. This is demonstrated by the often-received remark by crypto-enthusiasts that NFTs are a nonsense as one can simply click 'save image

[543] I italicise the word 'may' here because the Court refused to provide Leaf with a remedy because there was a five-year delay before he brought the claim. See ibid 92: [Contracts 'cannot be kept open and subject to the possibility of rescission indefinitely.'] (per Jenkins L.J.).
[544] Carolyn Hoffelt, 'The Value of Art in the Shape of Nfts: One Step Closer to Perfect Provenance, Market Transparency, and Access to Profit' (2023) 63 Jurimetrics: The Journal of Law, Science & Technology 355, 356.
[545] Saskia Hufnagel and Colin King, 'Non-Fungible Tokens: Art and Crime in a Virtual World' (2023) 5 Criminal Law Review 338, 345.

as..' and thus acquire ownership over the digital image.[546] It can therefore be expected that several copies of digital art will be available around the internet at any given time which are unconnected with the original author of the works. This becomes problematic where a copier sells the image as though it is the original, and then that image is innocently sold on to another. Under the doctrine of innocent misrepresentation, the harmed party may receive damages if the crypto-asset is not genuine unless the seller can show he had reasonable grounds to believe it was authentic.[547] Alternatively, he may rescind the contract.

The application of the doctrine of innocent misrepresentation here is mostly unproblematic. The reason is that in such transactions, the parties have formed an agreement outside of the blockchain. Additionally, any representations of fact are made in a plain language. For example, *Everydays* was sold through an auction at Christie's auction house in the same way that any other lot would be sold at auction. At this point, the natural language contract may be written under which the buyer obtains a right to the seller's performance with a correlative duty that the auction house performs by providing the original *Everydays* NFT. The duty is performed by the smart contract which may be written after the auction had concluded which would transfer the NFT to the buyer. If it had turned out that the work was not authentic, and a copy, the courts can assess the statements made to the buyer to determine whether there was in fact an innocent misrepresentation. If an innocent misrepresentation was made by the seller, the buyer may be entitled to rescind the contract. If the transaction took place entirely on the blockchain with minimal interaction between the involved parties, then no normative loss may arise upon which the buyer could sue as he would have bought the NFT according to its

[546] S Bonnet and Frank Teuteberg, 'Impact of Blockchain and Distributed Ledger Technology for the Management of the Intellectual Property Life Cycle: A Multiple Case Study Analysis' (2023) 144 Computers in Industry 103789, 17.
[547] Sale of Goods Act 1980, s 45(1).

aesthetic value and the price tag. Where the interaction involved no verbal interaction, the performance is merely based on how the asset is displayed on screen.

5.7.2 DASC misrepresentation

Blockchain technology enables any technologically savvy individuals to set up their own crypto asset project. Internet users are no longer 'passive consumers' of content, and may instead actively contribute and participate within the digital environment. The accessibility of the technology equally makes it easy for the creation of 'illegitimate' projects created to manipulate investors into spending their money on such projects. This type of project often uses DASCs to facilitate the transaction between its investors and its creators. It may also use a whitepaper which provides details regarding the transaction, including the total amount of crypto tokens to be issued, their value upon issuance, and the unique selling point of the asset.[548]

If an investor relies on the false information contained in the whitepaper, she may claim that the document contained a misrepresentation. For example, the $SQUID token project promised its investors through its whitepaper that they would have access to a virtual game in which they would be able earn more tokens.[549] This however was never the intention of those behind the project, who ultimately withdrew all the investors' funds and disappeared from all social media channels on which they were present. The idea of a play-to-earn game was an enticing element of the project, and so individuals exchanged their cryptocurrencies in return for $SQUID tokens in order to participate.

[548] The unique selling point is the function of the asset which compels individuals to invest in one crypto asset project over another. For example, this may include promises of a new blockchain or a playable game available only to investors.
[549] This is known as a "play-to-earn" token. To access the whitepaper, see < https://drive.google.com/file/d/1--4MDZ-2lNmh9KpZ0TfosVHkAPCuxD6Y/view>.

The elements of misrepresentation can be identified in a rug-pull. These projects fulfil the first criterion of misrepresentation as they make a false statement of fact by claiming that they are selling a 'tradeable' token, or that buyers of the same token will obtain access to a game. $SQUID particularly highlights this issue, as its creators never intended that investors could trade the token at a later date. To this effect, they coded an 'anti-dumping' mechanism into the smart contract that prevented the sale of the asset by anyone other than the project's administrators. They misrepresented the purpose of this mechanism, stating in the project's whitepaper that it served the legitimate purpose of preventing the rapid sell-off of the token by individuals trying to manipulate the market.[550] Thus, the misrepresentation is concealed within the code of the smart contract which other software developers or smart contract auditors may notice, but someone with minimal I.T. knowledge would not. Even a software developer may not understand the code of the smart contract because the coding language used differs between blockchains.[551] Although natural language is used in the whitepaper, the issue here is that the natural language expression and the code do not correlate. While the whitepaper promises a crypto-asset that functions and has some value, the smart contract enables the swift removal of that value by the asset's creators.

Once it has been established that the project creators made a false statement, it must be shown that the representation was material to the investor's decision to purchase the token. To be sure, an investor may not have relied on the statement contained in the whitepaper or smart contract and instead purchased the token based on general excitement within the crypto market. However, he may have been interested in a token if it had an underlying unique selling point such as if it consisted of a new blockchain, or if it was accompanied by a playable game. These

[550] i.e. the anti-dumping mechanism was pitched as a benefit to investors, and not as a device to assist the creators with fraud.
[551] Tan Shao Wei, 'Transnational Transactions on Cryptoasset Exchanges: A Conflict of Laws Perspective' [2022] Singapore Journal of Legal Studies 384, 390.

benefits are often communicated expressly through a crypto asset's whitepaper or website, and are sometimes material to an investor's decision as he views it as an opportunity to invest in new blockchain-derived technology. Alternatively, he may not be interested in the technological benefits of the project and may just seek a profit by trading the token later. Nonetheless, there is an implied representation that the token would be, at least, tradeable.[552]

Finally, the investor must have relied on statements regarding the crypto asset. This is essentially a question of causation, and whether the representation caused its recipient to enter into the agreement. This can be determined by asking whether the investor would have purchased the crypto asset even if he had not received the representation.[553] This is difficult for investors to prove because the transaction is facilitated by a decentralised, anonymous smart contract. As such, there is no communication between the project administrators and the investor prior to the transaction, and instead, the exchange is automated once the investor enters his cryptocurrency into the smart contract. Therefore, it is difficult to ascertain whether the investor truly relied on the representation as there is no communication between the parties to determine whether he even attributed any significance to the representation.

Even if a harmed investor successfully argues that he has suffered due to a crypto asset developer's misrepresentation, recovering his losses may be difficult due to the immutability of the smart contracts used to facilitate the rug-pull. Once he enters his consideration into the smart contract, the programme is executed, meaning the assets are permanently swapped and the transaction is recorded on the blockchain. The fact that many rug-pulls are conducted by anonymous parties creates additional challenges here. For instance, the identity of those behind the $SQUID token discussed above were never ascertained. Similarly, the true identity of the

[552] There is, of course, no right to earn a profit through speculative investments. The token should however serve its basic purpose in being a tradeable asset.
[553] Peel (n 308) 422.

creators of the 'Morgan DF Fintoch' rug-pull project was never discovered. That project claimed that it was owned by the giant American bank Morgan Stanley which prompted the bank to publish a statement declaring they were not affiliated with the project.[554] The project also used professional headshots of an actor to depict their CEO.[555] It remains unclear as to who was in fact behind the project. These two factors therefore affect the way in which the doctrine of misrepresentation can respond to DASCs demonstrated by rug-pulls which typically use this type of smart contract.

Evidently, a rug-pull transaction does not involve the genuine consent of the offeree in entering the exchange. The parties' unified relationship is formed based on a lie, and as a result, the offeree is worse off than what he should be. Under corrective justice, the courts may restore equilibrium in the parties' holdings. Rug-pulls are unfair interactions against which corrective justice militates. The reason for this is that the holdings of the rug-pull perpetrator is greater than they ought to be, and the investors' holdings are smaller than they must be.[556] The rug-pull transaction may be expressed in the following terms.

The rug-pull perpetrators actions may not be consistent with the freedom of the investors in determining their purposiveness. In buying a crypto asset, the investor often seeks a cryptocurrency or NFT with utility, a growing user base, and potential longevity. Frequently, rug-pull projects promise such outcomes with no intent to realise any of them. Yet, the investor acquires a right to the asset that was promised to them in the form that it was described. Usually, the asset is described as tradeable, or that it confers other benefits on the investor such as access to communities or opportunities. In making such pre-contractual statements, the rug-puller

[554] Morgan Stanley, 'Fintoch Important Notice' <https://www.morganstanley.com/content/dam/msdotcom/global-offices/pdf/Indonesia/Indonesia_Fintoch_Important_Notice.pdf> accessed 1 June 2023.
[555] Assad Jafri, 'Morgan DF Fintoch Goes Radio Silent after Rugging $31.6M' (*CryptoSlate*, 25 May 2023) <https://cryptoslate.com/morgan-df-fintoch-goes-radio-silent-after-rugging-31-6m/> accessed 9 June 2023.
[556] Weinrib, *The Idea of Private Law* (n 18) 115–116.

acquires a duty to provide the crypto asset as promised. Failing to do so is inconsistent with the investor's freedom as a self-determining agent.[557]

4.5.3.1 Misrepresentation or mere puffery?

Rug-pull perpetrators may argue in response to a plaintiff's claim of misrepresentation that they did not intend for her to rely on their statements.[558] However, this defence would not be available to them because even marketing stunts may amount to misrepresentations. An analogy can be drawn between crypto asset fraud and the classic case of *Carlill v Carbolic Smoke Ball*.[559] In that case, the defendant deposited £1,000 into an account to pay customers if the carbolic smoke ball did not work as a flu remedy. The Court found that this indicative of the smoke ball merchant's sincerity in its offer. A similar approach can be adopted in response to rug-pulls. The creators behind the project spend time and effort in designing its underlying infrastructure including writing the code for the smart contracts, and for the crypto token. In some projects, like $SQUID token, they may state that they add the 'anti-dumping' mechanism which can be construed as a form of protection for investors against value fluctuations. However, if the project is oriented in this way, its declarations arguably go beyond statements of intention or mere puffery and may be classified as binding offers, should the offeree choose to accept them.

Through the doctrinal recognition that a rug-pull is not the result of a 'mere puff', a corrective injustice may be recognised. A rug-pull bears some resemblance to the Carbolic Smoke Ball case as both rely heavily on 'aggressive advertising' practices.[560] The courts were able to

[557] ibid 122.
[558] As the defendant in *Peek v Gurney* (1873) 2 M & W 519 attempted to argue.
[559] *Carlill v Carbolic Smoke Ball* (1893) 1 QB 256.
[560] AWB Simpson, 'Quackery and Contract Law: The Case of the Carbolic Smoke Ball' (1985) 14 Journal of Legal Studies 345, 379.

provide Carlill with a remedy by first accepting that a contract existed between the two parties. This was done by reference to the defendant's placement of £1,000 in the bank. This set the defendant up with a duty, awaiting the plaintiff's acceptance which would provide her with the performance right, which if enforced, entitled her to £100. In a similar way, a rug-pull involves aggressive advertising practices such as promising excellent returns, among other benefits.[561] Therefore, the expressions used in rug-pulls may create a duty in the same manner that the courts found that the defendant in *Carlill* had.

Moreover, given that a rug-pull DASC is open to the world at large, Lindley L.J.'s final statement in his judgment may be applicable. He stated that 'the defendants must perform their promise, and, if they have been so unwary as to expose themselves to a great many actions, so much the worse for them'.[562] That is, anyone that suffered harm as a result of the defendant's action may also recover because the Court identified a basis upon which a contract could be found. All the factors of corrective justice were present; a plaintiff-defendant connection, a normative gain by the defendant and a normative loss by the plaintiff, and the correlative right and duty.

5.7.3 DAO misrepresentation

Given that DAOs are formed using a web of smart contracts, one of those smart contracts may result in liability for misrepresentation (whether it be fraudulent, negligent, or innocent). In this section, we turn to the concept of misrepresentation and whether DAOs may include the central criterion for liability for same: that there must be a false statement of fact made by the offeror

[561] Lin William Cong and others, 'The Dark Side of Crypto and Web3: Crypto-Related Scams' (14 February 2023) 10 <https://papers.ssrn.com/abstract=4358572> accessed 16 January 2024.
[562] *Carlill v Carbolic Smoke Ball* (n 532).

to the offeree.[563] A smart contract may be voidable only if the offeree can identify a statement which is decisive rather than one of opinion, or intention. By permitting the recipient of a misrepresentation to void the contract if she so elects, the doctrine of misrepresentation instantiates corrective justice by returning the parties to their pre-transaction position through the remedy of rescission or through damages.[564]

The need for the doctrine of misrepresentation arises, for example, where a DAO is used to perpetuate fraud against its other participants. For instance, a DAO's participants may submit, and vote for, funding proposals for projects that do not exist, and instead pocket the expended cryptocurrency themselves.[565] These proposals may be outlined natural language on the DAO's community forum before the transaction is formalised in a smart contract that is connected to the voting mechanism.[566] As the voting mechanism is linked to the smart contract, the latter may be coded to identify that the vote has passed, and if so, will automate payment to the recipient.

The proposal may be the basis for the plaintiffs' claim as this constitutes a false statement of fact. Although it has the appearance of a statement of intention, the proposer has actually misrepresented his mind in the manner that Bowen L.J. discussed in *Edgington v Fitzmaurice*.[567] If a participant misrepresents his intentions, the courts will construe the representation as one of fact.[568]

---

[563] *BS & N Ltd (BVI) v Micado Shipping Ltd (Malta) ('The Seaflower') (No 2)* [2000] CLC 802, 807: ['At the risk of stating the obvious, in order to set up a case of misrepresentation, it is necessary at the outset to establish by evidence that a representation of fact was made to the representee'] (per Timothy Walker J.).
[564] Weinrib, 'The Corrective Justice of Liability for Unjust Enrichment' (n 29) 168 (see particularly fn 1); See also: Herian (n 192) 29.
[565] 'What Can Go Wrong with DAO Investments, and How Should Investigators Respond?' (*Quantuma*, 15 February 2025) <https://www.quantuma.com/insights/what-can-go-wrong-dao-investments-and-how-should-investigators-respond> accessed 2 April 2025.
[566] On the mechanics of the DAO proposal, see 'How to Structure DAO Proposals and Build Proposal Processes' (*Aragon*) <https://www.aragon.org/how-to/structure-dao-proposals-and-build-proposal-processes> accessed 2 April 2025.
[567] *Edgington v Fitzmaurice* (1885) 29 Ch Div 459.
[568] ibid 483.

However, the DAO contract rests uneasily within the bilateral framework of corrective justice where misrepresentation is concerned. The smart contract is between the DAO's participants and the recipient project. However, the misrepresentation concerns a transaction between the participants and the DAO's treasury. The reason is that by submitting the proposal to the forum, the malicious participants aimed to induce the genuine participants to vote to execute the smart contract. Consequently, the genuine participants may not be able to claim on the basis of the misrepresentation.

5.8 Frustration of smart contracts

5.8.1 Frustration and Force Majeure in Bilateral Smart Contracts

Frustrating events are likely to be more common in smart contracts than conventional contracts because their execution is left to computer code, therefore increasing the probability of events beyond the parties' control.[569] A smart contract can generally be frustrated if a supervening event arises between the time of its formation and prior to the full performance of its terms. The question that arises is whether such frustration can occur in relation to bilateral smart contracts, wherein the parties have a natural language agreement, but which is executed using code. Take for example the use of smart contracts by companies for automatic payment when a ship delivers goods at the specified port.[570] For instance, the parties in *Tsakiroglou & Co v Noblee and Thorl* may have used a smart contract to manage their transaction had blockchain technology been available at the time. In that case, the parties had contracted for the shipment of cargo via the Suez Canal.[571] However, due to the Suez Crisis, the ship was unable to pass through the Canal, and had to divert through the Cape of Good Hope. The contract was not

[569] Kevin Nathaniel and Samuel Tey, 'Can Smart Contracts Outsmart the Law: The Law of Contract in Light of Smart Contracting' (2022) 2022 Singapore Comparative Law Review 93, 104.
[570] A common use-case for smart contracts appears to be in the shipping industry. *See* Filatova (n 19) 223.
[571] *Tsakiroglou & Co v Noblee and Thorl* [1961] 2 All ER 179.

held to be frustrated as it merely made the contract more onerous to perform, but not impossible. The Court considered that the cargo was non-perishable and therefore the longer duration was not a frustrating factor. Nonetheless, if this shipment was made in 2025 rather than 1961, the parties may have opted to execute their agreement using a smart contract which would automate payment once the ship arrived at its destination. In practice, the parties could do this using an 'internet of things' device in the form of a sensor which recognises that the ship has docked and unloaded the goods.[572] In this example, the deadline for delivery is coded into the agreement and Tsakiroglou would be automatically penalised for late delivery. The code in the smart contract may begin to charge 10% interest for each day that passes after the deadline.

The problem here is the inflexibility of the smart contract. Although the parties have established *on paper* the terms of their agreement which a human may recognise as frustrated by the supervening event, the coded component of the contract may not. In this instance, had the parties been dealing in perishable goods, their contract may have been frustrated. Yet, the the paper document and coded programme become misaligned and no longer 'speak' to one another. The natural language agreement provides that the plaintiff will deliver the goods to the defendant, but this becomes impossible. However, the smart contract cannot determine impossibility in the same way that the courts may. Consequently, the parties will have to endure the smart contract's performance because smart contracts may not adjust in response to unpredictable events.[573] The smart contract can only adapt if it was coded to recognise a particular event, meaning that the supervening event would be foreseeable to the parties. If this is the case, the doctrine of frustration would have no role in discharging the parties of their

[572] Filatova (n 19) 229.
[573] Durovic and Janssen (n 28) 74.

obligations.[574] Therefore, the interest clause coded into the smart contract would continue to deduct the money that had been placed in escrow in the smart contract.

The smart contract's inability to recognise a frustrating event is concerning from a corrective justice standpoint. In contracting, one party obtains the right to the performance of another. But if some unforeseeable event prevents that performance, it would be unfair to hold the parties to their bargain. If payment is made (as it is in the smart contract), then the lack of performance gives rise to another cause of action for breach of contract resulting from the smart contract's code and the inability of the parties to intervene to halt the payment process.

A similar outcome may be found in a bilateral smart contract created for a different purpose. For example, if a smart contract was created to facilitate the sale of tickets for a concert.[575] The attendees pay for their tickets by submitting their payment to the smart contract. The parties can use two smart contracts to ensure that the correct payment is made to the venue. The first smart contract is programmed to pay the venue a fee which they use to promote the event in the months between the formation of the agreement and the day of the concert. The second smart contract is coded to pay the venue a commission of 15% of the price of each ticket and the remainder is paid to the performers. Five days before the concert is due to take place, the venue is destroyed in a fire through no fault of either party.[576] The performers had put a significant amount of time and money into promotion and preparation for the concert. To recover the money spent, they would argue that there has been a breach of contract as the concert venue did not facilitate their performance. In response, the venue would argue that the contract was terminated due to the frustrating event. Ordinarily, the contract would be held to

[574] See section 5.3 for analysis on the requirement of unforeseeable supervening events in the doctrine of frustration.
[575] Aldweesh proposes a method to use smart contracts for the sale of electronic tickets. *See* Amjad Aldweesh, 'BlockTicket: A Framework for Electronic Tickets Based on Smart Contract' (2023) 18 PLOS ONE e0284166.
[576] The absence of fault makes the doctrine of frustration itself sit uneasily with corrective justice. See Weinrib, *Corrective Justice* (n 8) 188.

be discharged in such an event as it has become impossible to perform due to the destruction of its subject matter; the venue.[577] But in this instance, it would be difficult to terminate the smart contract from a technical standpoint, again resulting in one party paying for the others' performance even though performance has become impossible.

Although there is no fault by either party resulting in a corrective injustice, the smart contract here no longer reflects the will of the parties because the subject matter of the agreement no longer exists. The venue itself had a duty to facilitate the concert. At most, they may have partially performed their end of the bargain if they had promoted the event. The contract is voidable only from the point of the frustrating event and the venue is entitled to keep the payments for upholding its duty to promote the event. However, it did not (again, through no fault of its own) uphold its duty to facilitate the event. Given the deviation from the original purposes which the parties had in mind, discharging the parties of their correlative rights and duties would ensure corrective justice by ensuring the contract is not performed.

However, the use of a smart contract in the agreement prevents the easy discharge of the parties' obligations if a frustrating event occurs. Although the doctrine may apply in principle, it may be difficult to apply in practice. The reason is that payment has already been transferred under the contract. In theory, the parties to a bilateral smart contract may collaborate to undo the effects of the smart contract's code.

Another issue is that the parties may not have planned for the event in the coded terms of the smart contract. In particular, the issue here is the inflexibility of smart contracts. Of course, the parties may not have expected that the venue would have burnt down between the contract's formation and the performance of the concert. In the natural language document, the parties can expressly determine what should happen if such an unforeseeable event arises by including

[577] Based on an application of the factually similar case of *Taylor v Caldwell* [1863] 3 B&S 826 to the hypothetical case here.

a force majeure clause in the contract. Using a force majeure clause, the parties may suspend their bilateral relationship on their own terms. Although the contract no longer achieves the parties' purposes, they may at least bilaterally clarify what is to happen to the relationship if their purposiveness faces risk because of some supervening event.

However, smart contracts lack the flexibility to account for a broad range of supervening events in the same way as traditional contracts. Take for example a standard force majeure clause:

> 'In the case of failure to perform this Agreement due to any force majeure, neither party shall be liable for such failure, and this Agreement shall be terminated automatically. In the case of failure to perform any part of this Agreement due to any force majeure, the party suffering from such force majeure may be exempted from corresponding liability to the extent of the impact of such force majeure. However, such party shall continue to perform other obligations under this Agreement which have not been affected by such force majeure. If such force majeure occurs after such party delays to perform this Agreement, it shall not be exempted from its corresponding liabilities.'[578]

Under a traditional contract, a force majeure clause can include general indicators as to the kinds of events under which non-performance will be excused, or it may state as in the above example that force majeure events broadly excuse both parties of performance. Under a smart contract however, these events will have to be defined in specific detail because computer code requires such precision if it is to accurately carry out the instructions set out by the parties.[579] While it might be sufficient to define a supervening event in broad terms as 'natural disasters' or 'pandemics', the smart contract must be provided with specific instructions. In relation to the above hypothetical, the smart contract's code would have to include a term accounting for

[578] Afterpattern, 'Examples of Force Majeure Clauses in Contracts' (*Afterpattern*) <https://afterpattern.com/clauses/force-majeure> accessed 11 July 2022.
[579] On the need for specificity in a smart contract's terms, *see* Sklaroff (n 181) 277.

an ‘act of God resulting in the destruction of the concert venue by fire’. Code accounting for an ‘act of God’ alone would be insufficient because programming language must be precise. A trusted oracle may then provide the information to the smart contract that the concert venue in fact no longer exists.[580] This could theoretically be achieved by the oracle if it is coded to scan for items by news sources local to the concert hall. The courts may then verify whether the oracle was correct in withholding the payment via the smart contract.

5.8.2 DASC frustration

The doctrine of frustration may apply to DASCs where supervening events render performance impossible or radically different from the terms contained in the code. Without any natural language agreement dictating what ought to happen in the face of an unforeseeable event, the doctrine of frustration may ultimately determine whether the parties’ transaction can be voided. Corrective justice seeks to restore the balance in the parties’ holdings as though the transaction had not been taken place. The doctrine of frustration typically intervenes before performance has occurred in order to free the parties of their future obligations. This does not prevent the doctrine from being corrective in its nature, however. As Weinrib argued, corrective justice does not only obligate the defendant to correct a wrong after it has happened, but also operates to prevent the wrong from extending into the future.[581] Although Weinrib was describing how injunctions may provide corrective justice by preventing the continuation of wrongs, the reasoning may also be applied to the doctrine of frustration. If a DASC becomes impossible to perform, the absence of performance may constitute a wrong because the plaintiff through the smart contract may receive a performance right.

[580] Brownsword, ‘Regulatory Fitness’ (n 17) 9.
[581] Weinrib, *Corrective Justice* (n 8) 94–95 (Weinrib describing the purpose of injunctions in delivering up corrective justice.).

To clarify, smart contract transactions may face events rendering their code impossible to completely perform. The types of supervening events that arise in the blockchain context will differ from those in the off-chain setting. One potential example is the failure or closure of a cryptocurrency marketplace that facilitates peer-to-peer transactions.[582] Users of such exchanges may not set out their terms in a plain language agreement and may instead favour a transaction that is purely expressed in code. For example, two parties' algorithms may identify one another and become an integrated transaction through an algorithmically manifested offer and acceptance. Before the smart contract can perform, the exchange suffers an outage after consideration has passed from one of the parties but due to the system failure, the promisee does not receive what she is owed under the smart contract.

The doctrine of frustration is relevant to the discussion of smart contracts for two reasons. First, system errors may prevent the smart contract from being performed. For example, where a cryptocurrency exchange crashes immediately before or during the execution of a smart contract for the purchase of cryptocurrency. During this period, the purchaser may have paid for the cryptocurrency, but may not have received the asset in time before the crash affects the transactions. In such a scenario, the parties may be freed of their correlative right and duty under the DASC. If they are not, the plaintiff may be said to have suffered a normative loss and the exchange a normative gain, in which case the plaintiff may sue the cryptocurrency exchange for breach of contract or specific performance. However, this is not desirable as the defendant had intended to perform as the DASC was coded specifically to do so. As the consequences have rendered it such that the transaction no longer conforms to the parties' mutual purposes for the DASC, they may be freed of their obligations to one another.

[582] UK Law Commission (n 134) para 5.163.

Another potential reason for the frustration of a DASC may that the subject matter of the smart contract may no longer be available. For example, the creator of a piece of digital art may want to sell their work in NFT form, so they set up a smart contract to facilitate the transaction. Unbeknownst to both parties, the NFT is no longer available as it has been misappropriated from its creator. Further, the NFT may be deleted entirely through a process known as 'burning' which permanently removes the crypto asset from circulation.[583] In this scenario, the purchaser places money into the smart contract which in turn transfers it to the seller. However, the purchaser does not receive the digital asset as it was not located in the wallet to which the smart contract was connected. Once again, the seller has realised a normative gain through his receipt of payment for an asset which has not reached the plaintiff. However, damages or specific performance may not be appropriate here because neither party has done or suffered any wrong. The reason is that the supervening event – the misappropriation and subsequent destruction of the asset – did not occur through the fault of either party.

However, the doctrine of frustration may be inapplicable where a smart contract has been vitiated due to technical error where such error was foreseeable.[584] Human-error often leads to mistakes in the source code of software resulting in minor or major faults with the programme. Thus, parties can reasonably expect that not all of their smart contracts will be successful due to oversights in the code, and therefore their transactions may fail as a result. This category of fault is better assessed through the doctrine of mistake. Similarly, a smart contract may fail due to one of the parties having an insufficient Bitcoin balance in their crypto wallet.[585] This however would not be a sufficient excuse to set aside a contract, and could in any case be anticipated and accounted for within the smart contract's code. However, technical faults may

[583] Benedict George, 'What Does it Mean to Burn Crypto?' (*CoinDesk*, 26 January 2022) <https://www.coindesk.com/learn/what-does-it-mean-to-burn-crypto/> accessed 24 January 2023.
[584] Giancaspro, 'Is a "Smart Contract" Really a Smart Idea?' (n 216) 833.
[585] Eric Tjong Tjin Tai, 'Force Majeure and Excuses in Smart Contracts' (4 May 2018) 12 <https://papers.ssrn.com/abstract=3183637>.

occur beyond mere coding errors which could not be foreseen, and this is where the doctrine of frustration becomes operable. This category of fault would be more difficult to foresee, detect and account for in the smart contract, and may include widespread internet outages or where a crypto asset exchange is inoperable due to a cyberattack.[586]

The supervening event – the cyberattack – must affect the 'nature of the outstanding contractual rights and obligations' of the parties in order to frustrate the contract.[587] The typical transaction on a crypto asset exchange involves a buyer and seller, both who are anonymous to one another represented only by their crypto wallet numbers. The seller may put up for sale an NFT relating to a digital image, which the buyer accepts by submitting the stipulated amount of cryptocurrency into the smart contract. The transaction is not processed immediately, and could take up to two hours before it is recorded on the blockchain.[588] In the intervening period, the decentralised exchange platform which facilitated the transaction, or the blockchain itself could be taken offline by way of cyber-attack or serious technical fault. As a result, the performance of the exchange is affected – and the buyer's cryptocurrency is transferred to the seller, but she does not receive the NFT in return. The rights and obligations of the parties are therefore impacted as the buyer does not receive the right to ownership of the NFT, to which she is entitled on the basis of the original smart contract.

If this transaction was facilitated through a bilateral smart contract in which both parties knew each other, they could simply create a new smart contract in order to complete the performance of the transaction. However, the transaction considered here is conducted through a

[586] ibid.
[587] *Neville and Sons v Guardian Builders* [1995] 1 ILRM 1, 2.
[588] The time it takes to process a transaction is context dependent. For more on blockchain transaction times, *see* Michael Pacheco and others, 'Is My Transaction Done yet? An Empirical Study of Transaction Processing Times in the Ethereum Blockchain Platform' [2022] ACM Transactions on Software Engineering and Methodology 40 <https://dl.acm.org/doi/10.1145/3549542>.

decentralised exchange, which renders it more difficult for parties to coordinate a second transaction as their identity is concealed to one another.

Thus far, I have argued that there is an increased likelihood that smart contracts will become vitiated. In a 'straightforward' bilateral smart contract transaction, the parties may form their agreement off-chain but use the blockchain to perform and memorialise the outcome of the transaction. Yet, even this type of transaction is prone to human-error or frustrating events (driven particularly by the use of technology to facilitate the transaction). However, the parties may overcome the vitiation of the bilateral smart contract as they may find each other in the non-virtual world and redo the transaction, ensuring to avoid any errors made previously. In contrast, parties involved in a DASC may find themselves in an uncertain position if their agreement is vitiated. This is particularly problematic due to the immutability and anonymity of DASC transactions. This means that in essence, parties may be stuck with an unsatisfactory result from the exchange. Additionally, it is difficult for courts to determine whether a DASC has been vitiated if there is no corresponding plain language form of the agreement. The smart contract programme will perform in accordance with its code, but the outcome may not reflect the parties' intentions. Without another source that corroborates the parties' intentions, courts may have to rely solely on the DASC's code. This however overlooks the human nature of transacting.

5.8.3 DAO frustration

A contract may be frustrated where the performance of the parties' obligations under the contract would be 'radically different' from that which they anticipated in entering the contract.[589] There are various ways in which a DAO's smart contracts may not function as they

[589] *Davis Contractors Ltd v Fareham Urban DC* [1956] AC 696, 728–729.

were coded, rendering the performance of the parties' obligations as radically different. The blockchain or platform upon which the DAO is hosted may suffer an unforeseeable malfunction, or undergo a fundamental change that renders its smart contracts moot such as a hard fork. Alternatively, DAOs broadly or a specific DAO may be banned by regulators, therefore interacting with them may become illegal.[590] Given that supervening illegality is also a basis for finding a contract as frustrated, it is possible that DAO participants will claim to have their obligations discharged for this reason.[591]

The classic example of a potentially frustrating event in relation to smart contracts and DAOs is the attack on *TheDAO*. I have referred to this event on a few occasions throughout this thesis already, but it is worth briefly recounting the facts as they pertain to the issue of frustration. *TheDAO* was the first well-known DAO and achieved some level of success given its novelty. The idea behind it was that *TheDAO* could 'benefit' its token holders by relying on the wisdom of the crowds to determine what investments it should make.[592] It raised approximately US$150 million without establishing a corporate form that would limit its liability.[593] However, an attacker identified a vulnerability in one of its smart contracts and exploited it to withdraw US$50 million from the DAO's treasury.

TheDAO attack shows the difficulty in achieving corrective justice through the doctrine of frustration in DAO smart contracts. Its investors bought its token so that they may participate in voting on potential investments. It is likely then that the US$150 million was earmarked for certain investments and for upgrading and maintaining the DAO. When its token-holders vote,

[590] For example, the Tornado Cash DAO was banned by the US Treasury Department's Office of Foreign Assets Control who proscribed users in America from interacting with it. See Amir Ghavi and others, 'A Primer on DAOs' (*The Harvard Law School Forum on Corporate Governance*, 17 September 2022) <https://corpgov.law.harvard.edu/2022/09/17/a-primer-on-daos/> accessed 15 November 2024.
[591] *Fibrosa Spolka Akcyjna v Fairbairn Lawson Combe Barbour Ltd* [1943] AC 32; However, the excuse of illegality as a basis for frustrating a contract has a functional underpinning as it seeks to promote the observation of the law. See Ewan McKendrick, *Contract Law* (14th edn, Oxford University Press 2021) 298.
[592] Kolber (n 426) 212.
[593] TheDAO maybe constituted a general partnership. See ibid 212.

they effectively set into motion the smart contract between the DAO's membership and the funding recipient. The interaction of seeking funding and providing funding establishes the mutual wills of the parties. From this point on, a liability connection is formed between them.

The problem that arises is due to the immutability of a DAO's smart contracts. Once the smart contract is entered on the blockchain, it may not be taken back. However, what would happen if the attacker was able to withdraw all of the funds from *TheDAO's* treasury? If this did happen, *TheDAO's* membership would be unable to fulfil their duties in providing funding to its successful applicants. As such, they may be liable under the contract and may owe damages for the breach of the contract because the applications have gained a right to performance by *TheDAO's* membership. However, this would seem unjust because it is now impossible to perform by way of the smart contract because there are no longer the funds to do so through no fault of the *TheDAO's* participants.

The norm dictating the unfairness of the transaction is based on the lack of foreseeability of the attack on the DAO. It constitutes an unforeseeable supervening event for which contract law may free the parties of their respective obligations under the contract. However, such a conclusion can only be reached if we accept that cyber-attacks are in fact unforeseeable. While there is a looming risk that any organisation with an online presence will be subjected to a cyber-attack, this does not necessarily mean that the attack is foreseeable to the involved DAO. Coding errors and security vulnerabilities that permit such attacks in the first place are difficult to eliminate.[594] In *The Sea Angel*, Rix L.J. stated that 'the less that an event, in its type and its impact, is foreseeable, the more likely it is to be a factor which, depending on other factors in the case, may lead on to frustration'.[595] Therefore, to be foreseeable, someone must have identified the vulnerability to the DAO's membership prior to the attack, or the attacker must

[594] Mik, 'Contracts in Code?' (n 170) 504.
[595] *The Sea Angel* [2007] 2 Lloyd's Rep 517 [127].

have forewarned that he intends to exploit the vulnerability in the code. Unless these conditions are present, the attack may impede the will of the victim DAO's membership because it no longer has the funds to carry out the transaction as it had intended. The effect of the doctrine of frustration would be to sever the connection between the parties, therefore releasing them of their correlative rights and duties to one another so that the DAO's membership does not need to perform.[596]

5.9 Conclusion

This chapter highlighted the ways in which smart contracting parties' consent may be defective, owing to a mistake, misrepresentation, or frustrating event. It argued that the courts may be better equipped to identify defects in consent in bilateral smart contracts, because these expressly set out the correlative rights and duties of the parties. Such smart contracting scenarios clearly identify the terms to which the parties mutually agreed. The question for the courts in this context is whether the smart contract code's performance was different from what the provisions contained in the natural language agreement. However, decentralised smart contracts obfuscate defects in consent because they are often expressed only in the form of computer code. Such code may not inherently include misrepresentations, and a mistake may be difficult to identify if the courts do not know precisely what the parties sought to achieve by using the smart contract. Therefore, the bilateral smart contract is more easily mapped onto contract law's concepts than its decentralised anonymous counterpart. Consequently, parties who suffer significant financial loss resulting from DASCs may not be able to recover through the courts. This concerns us because liability ought to rectify the injustice caused by one party against the other.[597]

[596] McKendrick, *Contract Law* (n 591) 296.
[597] Weinrib, 'Corrective Justice in a Nutshell' (n 13) 349.

6 The Limitations of Contract Remedies: Assessing Where Traditional Remedies Succeed and Fail in Smart Contracts

6.1 Introduction

Over the last several decades, commerce has been undergoing a digital shift. Transactions which mostly would have taken place face-to-face and concluded with a handshake are now facilitated online either on a peer-to-peer basis or through intermediary marketplaces like Amazon. The current iteration of the internet, Web 3.0, purports to displace intermediaries and bolster peer-to-peer trading so parties can transact without the oversight or approval of another organisation.[598] Its objective is achieved through blockchains and smart contracts. These technologies combined have purportedly negated the need for traditional contract remedies issued by the courts or through other forms of dispute resolution.[599] This argument is based on the idea that smart contracts cannot be breached or vitiated because they are coded to ensure performance and execution of their terms. However, to be unbreachable, a smart contract must also be complete.[600] This means that the smart contract will not perform as promised (where there is an off-chain agreement) if the code is not sufficiently coded to realise the parties' expectations. Additionally, as the previous chapter has argued, smart contracts can be vitiated because the human parties responsible for their creation can include mistakes and misrepresentations in their smart agreements. Additionally, these human parties are at the mercy of the technology upon which they rely, and as such, cybersecurity breaches or network

[598] Massimo Ragnedda and Giuseppe Destefanis (eds), *Blockchain and Web 3.0: Social, Economic, and Technological Challenges* (Routledge 2019) 2.
[599] Poncibò and DiMatteo (n 150) 118.
[600] Barbara Pasa and Larry A DiMatteo, 'Observations on the Impact of Technology on Contract Law' in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019) 342 <https://www.cambridge.org/core/books/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/observations-on-the-impact-of-technology-on-contract-law/E1B770025777FE5D08995215E381F2C4> accessed 6 November 2022.

glitches may render a smart contract incapable of performance. It is therefore not possible to say with confidence that smart contracts dispense with the need for contractual remedies altogether. Instead, they merely reduce the need for court-enforced remedies.

To be sure of this, it is necessary to emphasise that smart contracts do not fully remove humans from the contracting equation. The smart contract only becomes 'autonomous' once its developer has coded it with instructions as to how it should perform once it has been executed. Although it is technically true that the smart contract self-performs and self-executes, this is only possible if it is facilitated by a human party. The human parties to smart contracts labour under certain limitations which impede the contract's self-performance, such as their inability to anticipate future events that may cause the smart agreement to perform in a way that contravenes the parties' intentions.[601]

There exists a notion that smart contracts fully perform the terms of an agreement without human intervention and therefore do not require remedies.[602] This is based on the idea that the agreement is self-contained within the smart contract. In other words, the code is the entire agreement and will be perfectly performed provided that it performs at all. This chapter argues that this view is shortsighted and fails to account for the complexity of smart transactions. The parties may hold intentions beyond the smart contract's code that may not be accurately captured by the smart contract and will therefore require intervention by the courts.

The objective of these remedies should be to ensure fairness and equality of the parties through an examination of their correlative interaction. Although Durovic argues that the purpose of contract law generally is to ensure the fairness, and the protection of vulnerable parties in

[601] Poncibò and DiMatteo (n 150) 119.
[602] Jason Allen and Peter Hunn (eds), 'Techno-Legal Supertoys: Smart Contracts and the Fetishization of Legal Certainty', *Smart Legal Contracts: Computable Law in Theory and Practice* (Oxford University Press 2022) 261 <https://doi.org/10.1093/oso/9780192858467.003.0012> accessed 4 March 2024.

transactions, this overlooks the treatment of parties in corrective justice as equals.[603] As such, the social rank or moral character of the parties (i.e. their vulnerability) does not factor into the determination of liability, and thus a remedy.[604] Although computer-centric modes of transacting are 'indifferent to the fundamental legal principles, such as lawfulness, fairness, and protection of the weaker party', the remedy may be determined by the 'nature of the right infringed'.[605] Corrective justice, through contract law, has a role in repairing injustices that the defendant has caused to the plaintiff. In rectifying the wrong suffered by the plaintiff, the remedy is applied correlatively to both parties; the defendant's gain is removed *and* the plaintiff's loss is restored.[587] A wrong occurs when the defendant acts in a way that is inconsistent with the right of the plaintiff. That right is created through the acts of offer and acceptance.[588] There are an array of remedies at the courts' disposal to restore the plaintiff's right. And the principle of *ubi remedium, ibi jus* applies.[606] If there exists a right and a correlative duty within the parties' interaction, then corrective justice operates to vindicate the plaintiff's right.

The main remedies available to parties in contract law and equity are damages, rectification, rescission, restitution, specific performance, and termination. These remedies are different instantiations of corrective justice in operation because they either work to provide the plaintiff with the subject matter of the right or prevent an infringement of that right into the future.[590] However, the applicability of those remedies may depend on the type of smart contracting arrangement to which they are applied. In a bilateral smart contract, the right to be vindicated by the remedy is identified in the natural language document. The remedy may undo the

[603] Mateja Durovic, 'What Are Smart Contracts?: An Attempt at Demystification' in Zvonimir Slakoper and Ivan Tot (eds), *Digital Technologies and the Law of Obligations* (Routledge 2021) 121.
[604] Weinrib, 'Corrective Justice Symposium' (n 71) 422.
[605] Savelyev (n 215) 128; Weinrib, *Corrective Justice* (n 8) 149.
[606] This maxim states that 'where there is a right, there is a remedy'. See Timothy Chan and Kelvin FK Low, 'Post-Scam Crypto Recovery: Final Clarity or Deceptive Simplicity?' (2023) 139 Law Quarterly Review 379, 381.

consequences of the code in line with that right, or it may rectify the code so that it better aligns with it. Accordingly, the plaintiff may be permitted to recover damages where the defendant's conduct causes him to suffer a normative loss, the nature of which may be ascertained by looking to the natural language agreement. Alternatively, where the asset contracted for by the parties is unique (e.g. an NFT), the courts may order the specific performance of the smart contract in line with the plaintiff's right. However, if non-performance is brought about by a gap in the smart contract's code, the courts may have to order its rectification prior to its subsequent enforcement. Similarly, it is in principle possible to rescind a bilateral smart contract by referring to the plaintiff's performance right, however the immutability of transactions may practically bar the rescission of such transactions.

However, in a DASC where the code constitutes the entirety of the agreement, the right is both created and executed within the smart contract in code form. This renders it difficult to identify whether the code's performance warrants a remedy, and if so, what that remedy should be. Consequently, identifying the basis for damages, rectifying, or rescinding a smart contract may be difficult. Finally, DAOs provide a conundrum for the remedial question because they involve a multiplicity of parties, therefore a remedy may have consequences for other parties who are not directly linked by the smart contract to be remedied. However, injunctions have proven as useful remedies for preventing the continuation of wrongdoing even where transactions are entirely in code or where the parties are anonymous to one another.

6.2 Breach of contract and damages

The standard measure in contract law for breach of contract is expectation damages.[607] This remedy naturally follows from the nature of the right which the promisee obtains when he enters into a contract. It is through this remedy that corrective justice rectifies any transactional imbalance, and therefore may restore the status quo between the parties. This is accomplished by imposing a loss on the defendant, and a correlative gain on the plaintiff, thereby shifting the value of the performance back to plaintiff.

However, whether or not smart contracts can be breached is a disputed fact. Indeed, one of the unique selling points of smart contracts and blockchain technology is that they prohibit parties from breaching the agreement. For instance, Werbach and Cornell argued that smart contracts do not permit breach because the computers that comprise the blockchain network ensure performance of the agreement's terms.[608] They further argue that a plaintiff would have 'no one to sue' because blockchains are decentralised networks formed of nodes rather than people.[609] Similarly, Savelyev argued that remedies for breach including damages, penalties or specific performance, are irrelevant unless they are specifically included in the smart contract's code.[610] Essentially, as the argument goes, the architecture of smart contracts and blockchains ensure that parties do not deviate from their agreement because they may only act in ways permitted by the smart contract's code. Therefore, if Tom sells to Paul a *Bored Ape* NFT for 1 Bitcoin and Paul deposits the Bitcoin into the smart contract, the smart contract will ensure they both receive what they are owed.

However, these arguments are unconvincing because a smart contract can only ensure performance if it has been correctly and precisely instructed in its code. A smart contract is a

[607] See Chapter 2, Section 2.2.2.
[608] Werbach and Cornell (n 12) 332.
[609] ibid.
[610] Savelyev (n 215) 130.

piece of software, and software generally speaking is difficult to create. It is more difficult to write software which will exist in 'distributed execution environments' like the blockchain.[611]

A breach of contract may occur when a party fails or refuses to perform her part of a bargain or where her performance is defective.[612] Both of these forms of breach may occur in smart contract transactions. For example, one party may withhold performance by coding the smart contract so that it executes at a time other than that agreed by the parties. Alternatively, a seller may enter the incorrect quantity of a particular asset into a smart contract and therefore be in breach of an agreement earlier formed by the parties. If either of these eventualities arise, the plaintiff will suffer a normative loss and the parties' holdings will become unbalanced.

Additionally, the courts will hold in private and commercial transactions that breach has occurred if the performance is not precisely as agreed between the parties.[613] The reason may be that performance which does not align with the parties' agreement constitutes an infringement on the plaintiff's right, and is a breach of the defendant's correlative duty.[614] This is demonstrated by *Re Moore & Co Ltd v Landauer & Co*, where the parties entered a contract for delivery of 3,000 tins of fruit which were meant to be packed in tins of 30 each.[615] However, some of the crates contained 24 instead of the agreed 30 tins. The UK Court of Appeal found that this constituted a breach of contract because of the 'considerable difficulty' the respondent may endure by receiving goods that were not delivered as described.[616] Therefore, performance

[611] Mik, 'The Sense and Nonsense of Smart Contracts' (n 5) 11.
[612] Edwin Peel and G. H. Treitel, *The Law of Contract* (15th edn, Sweet and Maxwell 2020) [17-049] cited in Ewan McKendrick, *Contract Law* (Bloomsbury Publishing Plc 2023) 404 <http://ebookcentral.proquest.com/lib/kcl/detail.action?docID=7217736>.
[613] Mindy Chen-Wishart, *Contract Law* (7th edn, Oxford University Press 2022) 500; In Ireland, the 'sale by description' rule no longer applies in the consumer context since the enactment of the Consumer Rights Act 2022. As such, a minor breach like that in Re Moore & Co would not result in the termination of the contract if it were a consumer contract. However, this standard still applies in private and commercial transactions. See Cliona Kelly, 'Au Revoir to Merchantable Quality for Consumers—the New Consumer Sales Law in the Consumer Rights Act 2022' (2023) 30 Commercial Law Practitioner 32, 33.
[614] Weinrib, *Corrective Justice* (n 8) 152.
[615] *Re Moore & Co Ltd v Landauer & Co* [1921] 2 K.B. 519.
[616] *Re Moore & Co Ltd v Landauer & Co* [1921] 2 K.B. 519 at 525 (per Scrutton L.J.).

must produce the outcome to which the parties agreed when they formed their agreement. There must be no defects in performance as was the case in *Re Moore & Co* because the defendant may be in breach of the plaintiff's contractual right. The issue that is overlooked by various blockchain enthusiasts is that smart contracts may include performance defects that would result in a breach of contract. Alternatively, one of the parties could opt not to perform the smart contract at all. However, how the courts may determine if a smart contract has been breached will depend on its nature, such as a bilateral smart contract with a natural language agreement or a DASC or DAO which lacks such a definitive creation of the plaintiff's right.

6.2.1 Breach in bilateral smart contracts

On the simpler side, bilateral smart contracts pose little challenge to the law as to what constitutes breach of contract. To determine whether there was a wrongful infringement of the plaintiff's right, the courts need simply look at the written agreement to which the parties mutually assented. Contractual breach may occur because the smart contract's code equips the defendant with the means necessary to conduct such breach. A hypothetical may help demonstrate the point. For example, a musician may agree to transfer the copyright over her music to another party in exchange for 1 Ether cryptocurrency.[617] In the natural language agreement, the parties stipulated that the transfer of the copyright would occur immediately from the point of the smart contract's execution. Once the transfer has occurred, the plaintiff obtains a portion of the royalties according to the number of times the music is streamed on digital platforms like Spotify. The defendant may decide that she does not want to proceed with the agreement if, for example, the music becomes popular once again. As such, she may

[617] For example, see Kate Irwin, 'Rihanna Producer Sells Royalties to "Bitch Better Have My Money" as NFTs' *Decrypt* (9 February 2023) <https://decrypt.co/120973/rihanna-producer-sells-royalties-to-bitch-better-have-my-money-as-nfts> accessed 13 March 2024.

maximise her profits if she retains her ownership of the copyright. Alternatively, she may decide to sell copyright ownership to another buyer for 2 Ether, a new price that reflects the increased popularity of the music.[618] The economic incentive would influence her to breach the agreement. This may be achieved in two ways.

In a conventional contract setting, the defendant could simply withhold the copyright notwithstanding that the parties had already agreed to the exchange. When the parties use a bilateral smart contract (where agreement happens prior to the smart contract's execution), the defendant may not write the smart contract software. This equates to the non-performance of the natural language agreement by the defendant, thereby infringing the plaintiff's right to the copyright. Alternatively, the defendant may write the smart contract but in so doing set an unrealistic date for performance (e.g. 10 October 2100). This way, the defendant retains the copyright into the distant future in breach of the terms of the parties' agreement, and the plaintiff would not receive the benefit of the exchange.

In the above bilateral smart contract transaction, the courts have the benefit of the written agreement which they can scrutinise to determine whether breach had occurred. The defendant undertook to provide the copyright by 10 October 2024. The courts may hold that she was in breach of the contract because of the late or non-performance of the agreement, thus permitting the plaintiff to sue for damages.[619]

The discussion of contractual breach coincides with that of damages because it is through the award of damages that the courts can quantitatively cure the loss incurred by the plaintiff due to the defendant's conduct.[620] Particularly, corrective justice justifies the expectation measure of contract damages because the defendant has normatively transferred a right to the plaintiff

[618] 1 ETH is worth €3566 at the time of writing, therefore the initial agreement was worth €3566 to the musician. It may be more efficient for her to sell the copyright ownership for 2 ETH at €7132.
[619] Chen-Wishart, *Contract Law* (n 586) 503.
[620] Weinrib, *Corrective Justice* (n 8) 94.

based upon which the plaintiff is entitled to defendant's performance.[621] The objective of damages then is to place the plaintiff in a position as though the defendant had performed according to their mutual agreement.[622] The plaintiff may accordingly recover the value of the 1 Ether which he paid for the copyright to undo the infringement to his entitlement under the bilateral smart contract.

6.2.2 The DASC and the inadequateness of damages

There are instances where damages may be an unsuitable remedy for the injustice caused by way of a smart contract. Particularly, it is difficult to determine the suitability of damages if the identity of the party cannot be ascertained. *Osbourne v Persons Unknown* is an example of such a scenario. In that case, the defendant gained unauthorised access to Osbourne's crypto asset wallet operated by MetaMask. Having successfully gained access, he transferred from her wallet two NFTs to a second wallet and subsequently to a third and fourth wallet. Osbourne sought an interim freezing order to prevent the further dispersal of the assets to other wallets because each time the NFTs were transferred made them more difficult to trace.

There are two reasons why the smart contract in that case is a DASC. Firstly, the defendant could not be identified because the blockchain provided a veil of anonymity. Secondly, the smart contract was entirely in code and immutable. HHJ Pelling found that damages were unsuitable because the defendant's identity was unknown and therefore their ability to pay even modest damages to the plaintiff was unknown.[623] Although, the defendant was potentially identified by the time of the third interim judgment in the *Osbourne* debacle by identifying

[621] Botterell (n 15) 110.
[622] Adams and Brownsword state that the courts have long determined damages for breach of contract based on the expectation interest of the harmed party. See Adams and Brownsword (n 175) 175. See also Parke Bin Robinson v Harman (1848) 1 Ex Rep 850, 855 (per Parke B.): '[The claimant] is, so far as money can do it, to be placed in the same situation, with respect to damages, as if the contract had been performed.'
[623] *Lavinia Deborah Osbourne v Persons Unknown* [2022] EWHC 1021 (Comm) [18].

their crypto wallet and its associated email address and social media username. Moreover, the assets in this dispute were deemed by the Judge to be unique rather than generic. The reason is that they were non-fungible tokens of 'personal and unique value' to the plaintiff as the were part of a collection where the earnings from the sales were used to fund scholarship and mentorships for women seeking careers in finance.[624] In sum, damages were held to be an inadequate remedy and the Court instead stated that an injunction would be readily granted in such circumstances.[625]

That an injunction could be granted in this case shows that corrective justice may still prevail in some circumstances where the parties use a DASC. The reality is that damages may not always be an appropriate means to rectify the losses suffered by the plaintiff in a specific transaction. In this instance, the two misappropriated NFTs were worth an approximate total of £4000 but they had a sentimental value to the plaintiff but damages in that amount would not rectify her loss if the NFTs were not returned. An injunction preventing the defendant from further transferring the NFT to other wallets or people is most appropriate in these circumstances.

One potential objection to injunctions as a means to achieve corrective justice that that they prevent future wrongdoing rather than correcting a wrong that has occurred. However, in this instance and more broadly speaking, DASCs are already executed, and therefore the plaintiff has already suffered the wrong. Therefore, the reason is found in the correlativity of the parties' interaction. Because the smart contract was executed illegitimately, the defendant infringed upon the plaintiff's right by trying to take away that which he did not own. The injunction therefore vindicated the plaintiff's right by ensuring the defendant did not impinge on the

[624] Cormac Kilkenny, 'Case Note: Osbourne v Persons Unknown and Ozone Network Inc t/a OpenSea Inc [2022] EWHC 1021 (Comm)' (2023) 30 Commercial Law Practitioner 17; Boss Beauties, 'Boss Beauties Make History At The New York Stock Exchange' (*Medium*, 27 October 2021) <https://bossbeauties.medium.com/boss-beauties-make-history-at-the-new-york-stock-exchange-715784cbb199> accessed 2 July 2022.
[625] *Lavinia Deborah Osbourne v Persons Unknown* (n 596) [18].

plaintiff's freedom by misappropriating her NFTs.[626] The injunction protected her right by preventing the defendant from further distributing the NFT so that it becomes unattainable by the plaintiff. In so doing, it prevented the wrong from being extended into the future.[627]

However, the Court had to overcome some procedural obstacles before it could grant the injunction. Specifically, it must be clear that the unknown defendant will be identified in the future before an interlocutory injunction could be granted.[628] To identify the defendant, the Court at first relied on Ozone Networks as it was the intermediary who operated the marketplace through which the relevant NFTs were exchanged. The Court hoped that Ozone would provide information regarding the unknown defendant pursuant to a Bankers Trust order. However, this was not guaranteed as Ozone were located in the United States; outside the jurisdiction of the English courts, meaning that the Bankers Trust order could not be enforced against the Ozone. This highlights the *potential* procedural challenges to obtaining corrective justice because a private law dispute requires both a plaintiff and a defendant. In DASCs, it may be difficult to identify the defendant because their identity is obfuscated by the anonymity provided by the blockchain. Ultimately however, Osbourne acquired the information necessary to identify the defendant by enlisting a cybersecurity investigator.[629] Therefore, although it is difficult to identify the correlative defendant involved in a DASC, it is not impossible.

Another example of a DASC where damages were deemed inadequate by the Court is *AA v Persons Unknown*.[630] The unknown defendant in that case obtained 109.25 Bitcoin by holding several customers' computers hostage by infecting them with ransomware. To free their computers, they had to pay a ransom in Bitcoin, a useful medium of exchange in this scenario

[626] Weinrib, *Corrective Justice* (n 8) 94.
[627] ibid 95.
[628] *Cameron v Liverpool Victoria Insurance Co Ltd* [2019] UKSC 6; Gary Watt, *Equity and Trusts Law* (Oxford University Press 2021) 487.
[629] *Lavinia Deborah Osbourne v Persons Unknown* [2023] EWHC 2974 (KB) [11].
[630] *AA v Persons Unknown* (n 94).

due to its untraceable quality. However, the reason damages were unsuitable differed to *Osbourne*. Bryan J. stated that it was appropriate to grant an injunction instead of damages because the 96 Bitcoins that were stolen could be dissipated by the attacker. Once again, although damages may place the plaintiff in a position as though the defendant's wrong never occurred, the injunction prevents the wrong from continuing into the future.

6.2.3 Breach of DAO smart contracts

A defendant breaches a contract when he does not fulfil his duty to perform in accordance with the plaintiff's right to performance (i.e. a violation of the plaintiff's right, in Weinribian terms), without any excuse for his failure to perform.[631] Breach may take various forms ranging from the express, vocalised refusal by the defendant to perform to conduct amounting to his outright non-performance or defective performance. There are various reasons why it may be difficult for a DAO participant to claim that another party has infringed his right so as to warrant the award of damages. If this correct, the parties' holdings may not be equilibrated so as to correct the normative loss of that participant.

The first reason is that there are a multiplicity of interacting smart contracts within the overall nexus that constitutes the DAO. A party situated in the DAO may fail to perform because of an externally linked protocol rather than a smart contract situated within the DAO itself. External protocols may be used to bring about the performance which the plaintiff may expect according to the right he has obtained through the smart contract. These external protocols may take the form of auxiliary smart contracts which enable the DAO's participants to swap tokens, manage collateral, or to interact with DeFi applications that are external to the DAO. With all these smart contracts forming a complex web of interactions both within and outside of the DAO, it may become unclear as to what contract exactly is being breached. The plaintiff may be

[631] Weinrib, *Corrective Justice* (n 8) 166; McKendrick, *Contract Law* (n 591) 380.

identified as she is the one who suffers some form of normative loss resulting from the transaction. For example, she may notice a decrease in her holdings resulting from the execution of a particular smart contract situated within the DAO but had not obtained the object of the smart contract after its supposed performance. However, identifying the party who made a normative gain within the messy web of autonomous interactions may prove difficult. This necessarily upsets the form of corrective justice because the private law dispute involves a plaintiff and a defendant who are linked by a single liability.[632] Within the DAO, the normative loss incurred by the plaintiff may be the result of cascading failures due to the interdependency of the smart contracts on the DAO. For example, a stablecoin mechanism within the DAO may malfunction, resulting in the deviation of its value from its reference asset.[633] Smart contracts situated downstream dependent on the stablecoin may result in the failure to perform the transfer expected by the plaintiff. However, determining where the breach lies involves examining the chain of smart contracts which itself will be a difficult task because each smart contract depends on various inputs and conditions maintained by others. As such, there may not be a bilateral nexus sufficient to ground the plaintiff's claim.

The second difficulty lies in identifying the terms of which the defendant has purportedly breached. In a conventional contract or bilateral smart contract, the plaintiff may refer to the plain language agreement to show that a breach has taken place. For example, in *Robinson v Harman*, the defendant wrote to the plaintiff offering him a 21-year lease of a house but subsequently reneged. The plaintiff could rely on the wording of the letter to determine the content of the performance right which had been breached. The words there stated that the

[632] Weinrib, *Idea* (n 14) 63.

[633] A stablecoin is a form of cryptocurrency whose value is attached to a more stable asset (such as the US dollar). De-pegging means that the value deviates from the asset to which the stablecoin has been 'pegged'. De-pegging may happen because of surges in supply and demand, market volatility, or network issues and hacking. See 'Stablecoin Depegging: The What and Why' (*Kraken*, 5 December 2024) <https://www.kraken.com/learn/stablecoin-depegging> accessed 17 December 2024.

defendant would 'grant and deliver to the plaintiff a good and valid lease of a certain dwelling-house, and other hereditaments and premises in the agreement mentioned, for a term of twenty-one years from the 29th day of September then next ensuing, at the yearly rent of £110'.[634] The plaintiff may claim that, because the defendant did not perform in line with the content of the letter, he was in breach of the parties' contract. However, the identification of terms is not so straightforward in a DAO smart contract because rights and duties of the smart contracts contained therein are embedded in their code that deterministically executes according to rules that the plaintiff may not fully comprehend. Misalignment between what the parties intended and how the code subsequently executes may obscure whether any breach had in fact occurred.

If it is difficult to identify breach, it will also be difficult to provide the sufferer of the loss with a remedy in damages. Without any term to reference, the loss is factual rather than normative, and as such, corrective justice may not necessitate a remedy due to the lack of any breached norm.[635]

6.3 Specific performance

Damages are the primary remedy for contractual breaches; however, the courts have discretion to grant the equitable remedy of specific performance where damages would be inadequate. In *Beswick v Beswick* for example, the House of Lords stated that specific performance should only be ordered if it would 'do more perfect and complete justice' than if damages were awarded.[636] In particular, specific performance rectifies the injustice resulting from the defendant's breach of contract by requiring the defendant to perform as he had promised.[637]

[634] *Robinson v Harman* (1848) 154 ER 363, 363.
[635] Weinrib, *Idea* (n 14) 116.
[636] *Beswick v Beswick* [1967] 3 WLR 932, 90.
[637] Drawing on Kant's formulation of right, Weinrib states that under an order for specific performance, the plaintiff is not entitled to the thing for which the parties contracted, but to the performance of the contract. See Weinrib, *Corrective Justice* (n 8) 154.

However, specific performance is only available as a remedy where the subject matter of the contract is unique and cannot be substituted with damages. Indeed, specific performance may be the best way to attain justice between the parties where the subject matter of the contract is 'unique and particularised'.[638]

Such novel subject matter for which orders of specific performance were made in the past include china jars 'of unusual beauty, rarity and distinction', or an old but unique ship.[639] Therefore, if the subject matter of the contract cannot simply be repurchased elsewhere, the courts may grant an order for specific performance instead of damages. The copyright over a song that cannot be replicated due to intellectual property laws could therefore be sufficiently unique to warrant specific performance over damages. Music is, by its nature, one-of-a-kind. The remedy of specific performance can further be discussed in terms of cryptocurrencies and NFTs because the former tends to be generic and the latter unique.

To determine whether NFTs are sufficiently unique to warrant specific performance requires we ask what exactly an NFT's purchaser receives in purchasing the crypto asset? A well-known example of an NFT includes the 'Nyan Cat' token which sold for $580,000.[640] *Nyan Cat* was originally a viral YouTube video of a flying cat with a pop-tart body that received millions of views and was subsequently converted into GIF format and reposted all over the internet by various users. While there are replications of the video across the internet, the NFT itself is exclusive to its holder. The NFT is a token that represents ownership of the graphic rather than the graphic itself.[641] Therefore, if another person attempted to buy this NFT but the smart

[638] Botterell (n 15) 111.
[639] McKendrick, *Contract Law* (n 206) 902; china jars: Falcke v. Gray (1859) 4 Drew 651; old ship: Behnke v. Bede Shipping Co Ltd [1927] 1 KB 649.
[640] Jacob Kastrenakes, 'Nyan Cat Is Being Sold as a One-of-a-Kind Piece of Crypto Art' *The Verge* (18 February 2021) <https://www.theverge.com/2021/2/18/22287956/nyan-cat-crypto-art-foundation-nft-sale-chris-torres> accessed 14 March 2024.
[641] Juliet M Moringiello and Christopher K Odinet, 'The Property Law of Tokens' (2022) 74 Florida Law Review 607, 609.

contract for the transaction was breached, they would likely obtain an order for specific performance because only one NFT exists although there are many replications of the corresponding graphic available on the internet. The courts will focus on the fact that only one user in theory can hold an NFT at a time.

The remedial response would be different if the transaction was for the sale of cryptocurrencies because they are an asset that is widely available through various crypto-asset exchanges. For example, if a party entered a transaction to buy a Bitcoin that failed due to breach, damages would be the appropriate remedy because there are almost 20 million Bitcoins in circulation at the time of writing. Therefore, if the harmed party can recover the money that they lost in buying the Bitcoin, they will be able to enter another transaction with another seller of the cryptocurrency. Cryptocurrencies are not sufficiently rare to warrant specific performance.

In essence, smart contracts for the purchase of cryptocurrencies are akin to contracts for company shares that are publicly traded on the open market. The sale of such shares usually cannot be specifically enforced because damages will be sufficient and the cryptocurrency can be bought in a separate transaction via the open market.[642] It follows that the courts may be slow to specifically enforce a contract for sale of a cryptocurrency, especially one that is as widely available as Bitcoin, because it can be bought elsewhere.

6.3.1 Specific performance in bilateral smart contracts

However, specific performance will not be granted where a contract is too vague.[643] Though, one view of smart contracts is that they are not vague at all because computer code is written in formal language compared to its fiat counterpart which often contains vague notions of

[642] *Mills v Sportsdirect.com Retail Ltd* [2010] EWHC 1072 (ch), para 75.
[643] McKendrick, *Contract Law* (n 206) 904.

reasonableness and good faith.[644] Whereas fiat contracts often contain such vague terms to provide their drafter some flexibility in its performance, smart contracts use precisely coded terms to bring about specific outcomes. Given that the coded part of the bilateral smart contract cannot perform terms which are insufficiently precise, the natural language component should equally not include such open-ended terms. The question then is: who may perceive a smart contract as vague? Although the computer itself will be capable of reading and executing machine-readable code, a human party may have difficulty in comprehending the terms set out in the code. This includes judges, who may have to specifically enforce a contract according to its terms.[645]

Co-Operative Insurance Society Ltd v Argyll Stores (Holdings) Ltd is a good example of what does and does not constitute vagueness because the UK Court of Appeal initially held that a term was precise enough to be enforced but the House of Lords differed in its judgment.[646] The impugned clause in this case required Argyll Stores, a struggling business, to keep their shop open during business hours and to keep the storefront window 'dressed in a suitable manner'. According to the Court of Appeal, Argyll's obligations under an order for specific performance were sufficiently certain: that they would continue to operate the shop until 2014 or until they found a subtenant to take over the premises. However, the House of Lords found that the language of the covenant was too open-ended, and did not account for the amount of, or kind of trade, that the defendant had to undertake, nor did it state the location within the premises where trade was to be conducted. On this basis, the court refused to grant an order of specific performance because they are reluctant to grant specific performance where the term to be

[644] Edmund Schuster, 'Cloud Crypto Land' (2021) 84 The Modern Law Review 974.
[645] McKendrick, *Contract Law* (n 206) 920–921.
[646] *Co-Operative Insurance Society Ltd v Argyll Stores (Holdings) Ltd* [1998] AC 1; [1996] Ch 286.

enforced contains ambiguities, meaning that the courts do not know exactly what it is they are enforcing. This has ramifications for smart contracts because they may lack certainty.[647]

For example, an artist may sell enter an agreement with a buyer for the sale of her digital artwork in the form of an NFT. To do so, she sets up a smart contract which will automatically transfer the ownership of the NFT to the buyer when he submits 5 Ether to the smart contract. To execute the transaction, the buyer connects his crypto wallet to the NFT marketplace and sends the 10 Ether to the designated address. However, a bug in the smart contract causes the smart contract to malfunction, so the seller receives the Ether contract, but the buyer does not receive the NFT, meaning that the seller still holds the digital artwork. However, the courts may turn to the natural language agreement to determine the right of performance which would be satisfied by the smart contract's passing over of the NFT to the buyer. Had the smart contract existed only in code, the seller's correlative duty may be unclear. However, even with the natural language document in place, the specific enforcement of the same code would produce the same results, thereby infringing the right of the buyer once again. To correct the imbalance of the parties' holdings, the courts may first have to rectify the code of the smart contract (effectively creating a new smart contract due to the immutability of the first). Once the new smart contract has been established, the courts may require that it is enforced to ensure the transaction is executed in a manner that matches the parties' purposes.

One might argue that the courts should consider that the code did not perform as intended, and that the seller is now benefitting from the software without having to fulfil her side of the bargain. It follows that an order to have the code specifically performed would ensure that the buyer receives the asset for which he contracted. In other words, specific performance corrects the injustice between the plaintiff and defendant because the defendant undertook to perform

[647] Giancaspro, 'Is a "Smart Contract" Really a Smart Idea?' (n 126) 831.

by transferring the NFT to the plaintiff. His conduct is inconsistent with the plaintiff's right because he has not performed in the way that he had promised.

Yet, the 'code *is* law' proponents would hold that the transaction ought to be left in a state of incompleteness if this was the consequence of the smart contract's code.[648] Viewing code as an alternative to contract in this way is problematic for this reason. However, in the bilateral smart contract context discussed above, the performance right of the plaintiff may be objectively ascertained by the courts by drawing on their natural language agreement. However, turning back to the DASC, we can see how specific performance may lead to correctively unjust transactions if the courts adhere too rigidly to the 'code is contract' standard.

6.3.2 Specific performance and the DASC

The plaintiff in *B2C2 Ltd v Quoine Pte Ltd* sought an order of specific performance to have the trades reinstated after Quoine had unilaterally reversed them. The defendants argued that specific performance was the appropriate remedy because of the volatility of cryptocurrencies generally, meaning that it is difficult to ascertain their inherent value.[649] In turn, this would render it difficult to assess damages and thus specific performance would be the most appropriate remedy. However, The SICC stated that the courts are familiar with determining damages in relation to volatile assets and that cryptocurrencies are not unique in this regard.[650] Further, the Court stated that specific performance would cause Quoine substantial hardship because this would require Quoine to obtain Bitcoin at a significantly higher price than when the trades were made.[651] Both of these reasons are sufficient for declining to grant an order of

[648] De Filippi and Wright note the distinction between 'code *is* law' versus 'code *as* law'. The former means that rules are built into the code, including contractual rules. The latter refers to the use of code as a way to implement state laws and regulations. *See* de Filippi and Wright (n 148) 199.
[649] *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03, para 255.
[650] *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03, para 255.
[651] *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03, para 256.

specific performance because cryptocurrencies are not sufficiently unique and can be repurchased using the money owed in the form of damages. Additionally, it would be unfair to obligate Quoine to repurchase Bitcoin to return to B2C2 when its price had increased by approximately $2118 since the time of the transactions.[652] The Court was therefore correct to conclude that specific performance would not be appropriate here. As a general rule, cryptocurrencies and non-fungible tokens may often be the subject matter of DASCs. This may render it difficult for a plaintiff to obtain an order of specific performance against the defendant in such a contract.

Digressing from the doctrinal bar to specific performance caused by the ebb and flow of crypto asset prices, there is the fundamental problem of enforcing a code-only agreement. Although smart contracts are responsible for enforcing their *own* terms, the terms in a DASC must be carefully and precisely coded, otherwise they will fail to perform or will perform in a manner that is contrary to the will of the parties.[653] Given that code-only contracts require such specificity, they should *theoretically* manifest the parties' will accurately. However, this is not always the case as *Quoine* and other extra-judicial disputes indicate.

Even though the case centred on the doctrine of mistake and its applicability in trades facilitated by smart contract, the crux of the case is on what knowledge the parties had about the terms to which they had agreed.[654] Applied to specific performance, the question becomes whether the parties can possibly have sufficient knowledge of the meaning of a piece of code so that it can be specifically enforced? The answer is that it is unlikely that courts will specifically enforce a term within a smart contract if a natural language version of the term is

[652] Based on a calculation of the approximate value of Bitcoin on the following dates: [date of judgment] March 2019 – April 2017 [date trades were made].
[653] Sklaroff (n 181) 277.
[654] *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03, para 198. The questions posed by Simon Thorley I.J.: [How does one assess knowledge or intention when the whole operation is carried out by computers acting as programmed? Whose knowledge is relevant? At what date is this knowledge to be assessed?].

non-existent. One reason is that smart contracts are pieces of software, the 'language' of which may be unintelligible to non-programmers.[655]

The difficulty with enforcing a DASC is that the courts would be enforcing the same smart contract that led to the purported breach in the first place. To bring about justice in the transaction, the code in the smart contract would first need to be altered. This begs the question as to how the code should be changed if it is to reflect the parties' mutual will. The lack of any natural language agreement means that the code is the only reflection of their will. In some instances, it may be easier to determine what specific performance of the particular transaction ought to look like.

The *CryptoPunk #2386* incident is another example where specific performance would not instantiate corrective justice. To briefly recount the facts of that situation, *CryptoPunk #2386* was an NFT valued at US$1.5 million. It was bought by a user who executed a smart contract associated with a long-defunct NFT marketplace. Other users attempted to prevent the transaction but failed.[656] Had they been successful, the buyer may try to specifically enforce the coded agreement because he would obtain the asset for which he paid significantly below the market price.

If the terms of the smart contract are considered to be 'set in stone', then the courts may award an order of specific performance to the NFT's buyer.[657] However, this outcome would be correctively unjust, as was the executed transaction. The reason is that the seller suffered a normative loss, and the buyer suffered a normative gain because the offer may have been revocable due the passage of time. As such, the buyer and seller were not part of a unified transaction because the seller's offer was no longer valid. Consequently, the buyer did not

[655] Giancaspro, 'Is a "Smart Contract" Really a Smart Idea?' (n 216) 831.
[656] Packin (n 238).
[657] ibid.

obtain an *in personam* right to the seller's performance (in the form of the transferral of the asset).

6.3.3 Specific performance in DAOs

Specific performance is one method of providing to the plaintiff what she is owed in a manner that conforms to the requirements of corrective justice.[658] It eliminates the inconsistency with the plaintiff's rights by enforcing the defendant to perform his correlative duty under the contract. However, the plaintiff may face some of the difficulties identified in relation to breach of contract when it comes to seeking an order for specific performance.[659] There are some remedial challenges to specifically enforcing DAO smart contracts because of their decentralised, autonomous features. As such, vindicating the plaintiff's right through enforcement may be impracticable.

The DAO contracts contain terms that are encoded as computer instructions rather than plain language, resulting in an opacity that prevents those terms from being understood by the parties who interact with them. Any purported breach may simply be the smart contract performing exactly as it was programmed, even if its outcome was undesirable for the plaintiff. The idea of breach, which presupposes a party's failure to perform his duty under the contract, becomes a blunt doctrine for assessing DAO smart contracts. It may therefore be difficult to determine whether the plaintiff is in fact entitled to specific performance where the terms to be enforced are in the form of black box code.[660]

In addition, the web of interacting smart contracts and its external protocols may contain flaws that result in non-performance due to the breakdown of one of the contracts within the chain.

---

[658] Ernest J Weinrib, 'Civil Recourse and Corrective Justice' (2011) 39 Florida State University Law Review 273, 287.

[659] For the discussion relating to issues with correlativity and breach on contract in DAO smart contracts, see section 6.2.3.

[660] Gregory Klass, 'How to Interpret a Vending Machine: Smart Contracts and Contract Law' (2023) 7 Georgetown Law Technology Review 69, 91.

For example, a DAO may be set up to provide crowdsourced NFTs to purchasers. The crowdsourced assets are provided to the DAO by an external protocol. If the DAO stops paying the external protocol, and it stops sending new NFTs over, the DAO may default on its obligation under the smart contract. Even though the transaction is provided for in the contract's code, the smart contract may only issue an asset if there is one for the smart contract to locate within the DAO's collection. If the DAO's smart contract does not provide the end-user with the NFT for which she paid, she may try to specifically enforce the contract because NFTs are unique assets, meaning that damages may not be preferred. Nonetheless, identifying the specific smart contract responsible for the breach may be difficult in the mass of smart contracts that constitute the overall DAO. Given that the whole process is automated, and there is no centralised party responsible for the DAO's operation, it may be difficult to identify a defendant against which to claim for specific performance.

6.4 Rescission

Rescission instantiates corrective justice by setting the contract aside from the beginning, and placing the parties into their pre-contract position.[661] The courts may restore the parties to a position as though the contract had not been performed by removing the defendant's gain and returning it to the plaintiff.[662] It may be difficult to rescind a smart contract because once deployed on the blockchain, it is impracticable to delete a smart contract.[663] Further, once a smart contract is executed, it is not possible to halt execution and the agreement as coded will

[661] Paul Anthony McDermott, *Contract Law* (2nd edn, Bloomsbury Professional 2017) para 24.40.
[662] Weinrib, 'Corrective Justice in a Nutshell' (n 13) 349.
[663] The early literature on smart contracts discuss how they are impossible to delete from the blockchain once they are deployed on it, however it is technically possible to delete smart contracts by coding a 'self-destruct' function into the software. *See* Bill Marino and Ari Juels, 'Setting Standards for Altering and Undoing Smart Contracts' in Jose Julio Alferes and others (eds), *Rule Technologies. Research, Tools, and Applications* (Springer International Publishing 2016).

be fully performed.[664] Additionally, one or both parties may not realise that the code of the smart contract will not bring about the outcome that they intend. For example, one party may have intended to buy a *Cryptokitty* NFT but instead received a *Cryptopunk* because it was not clear on the face of the smart contract that the latter asset was involved in the transaction rather than the item they sought. Consequently, the equitable remedy of rescission will be brought to the fore in response to smart contracts because it enables courts to unwind a transaction *ex post*. If the content of a smart contract cannot be understood by its human recipients and also cannot be halted, the courts will increasingly have to determine how the harmed party can be remedied after performance has taken place.

Rescission involves the cancellation of a contract by one or both parties, but with the additional step of returning the parties to the position they would have been in had they never entered the contract.[665] The objective of rescission is to ensure the harmed party will be returned any advantages they delivered under the contract, reimbursed for any detriments they suffered, and are released from any obligations formed by the contract.[666] Finlay Geoghegan J. quoted Keane C.J. (as he then was, writing extra-judicially) in *Mackin v Deane* that rescission arises where one party breaches a term that is essential or 'goes to the root of the contract'.[667] Further, Keane C.J. stated that other instruments used in a transaction may also be set aside. Therefore, even if a smart contract only performs one part of a broader agreement, the smart contract could still be set aside where the breach is completely at odds with the spirit of the transaction.[668]

[664] Werbach and Cornell (n 12) 332.
[665] Marino and Juels (n 663) 153.
[666] David Capper, 'Remedies for Misrepresentation: An Integrated System' in Keith Rowley and others (eds), *Commercial Contract Law: Transatlantic Perspectives* (Cambridge University Press 2013) 389
[667] Ronan Keane, *Equity and the Law of Trusts in the Republic of Ireland* (Butterworths 1988) 254, cited with approval in *Mackin v Deane* [2010] IEHC 192 at para 35.
[668] Smart contracts are often used merely as a device to automatically perform agreements that the parties have already concluded. Filatova (n 19) 229.

The remedy of rescission is only available in a narrow set of circumstances including misrepresentation, mistake, undue influence and duress.[669] Where misrepresentation is involved, the contract is voided 'retrospectively and prospectively'.[670] Where a contract is rescinded because of the breach of an essential term, the parties are only liberated from their obligations to perform in the future and it does not apply retrospectively.[671]

In relation to smart contracts, the need for rescission will likely arise in relation to misrepresentations. However, a difficulty with fit between rescission and smart contracts is caused by the rule in *Seddon v North Eastern Salt*.[672] The rule provides that a contract can only be rescinded before it has been executed unless there is equitable fraud involved.[673] Therefore, smart contracts used to facilitate fraud may be rescinded but legitimate transactions may not because the harmed party may only become aware that rescission is needed post smart contract execution. For example, a smart contract may be used to purchase assets in the *Metaverse*, an immersive 3D virtual world where people can trade, socialise and work. It combines virtual reality (VR) and augmented reality (AR) to simulate a semi-realistic world in which users can meet other users who are represented by their 3D avatars.[674] The combination of the Metaverse and blockchain technology provides an opportunity to develop electronic commerce capabilities. Legal disputes may arise between parties when their intentions are not reflected in electronically facilitated transactions.

[669] Paul Anthony McDermott, *Contract Law* (2nd edn, Bloomsbury Professional 2017) [24.40].
[670] McKendrick, *Contract Law* (n 591) 287.
[671] ibid.
[672] *Seddon v North Eastern Salt* [1905] 1 Ch 326.
[673] *Seddon v North Eastern Salt* [1905] 1 Ch 326, 332.
[674] Jon M Garon, 'Legal Implications of a Ubiquitous Metaverse and a Web3 Future' (2022) 106 Marquette Law Review 163, 169.

6.4.1 Rescission of bilateral smart contracts

As previously stated, one cause for a contract to be rescinded is misrepresentation, be it fraudulent, negligent or innocent.[675] A misrepresentation may arise in a smart contract used for an exchange on the Metaverse. One of the primary ways to obtain ownership of assets on the Metaverse is through NFTs which authenticate a user's ownership over a particular digital item. To explain how a misrepresentation may arise on the Metaverse that warrants the rescission of a smart contract, a user may sell to another user a plot of virtual land. This is facilitated through the sale of an NFT that reflects ownership over the 3D model that is situated in the Metaverse. The holder of the NFT is regarded as the owner of the digital property. However, unbeknownst to the seller, the 3D model contains corrupted code that renders glitches in the display of the asset in the Metaverse. Due to the faulty code, the virtual 'textures' of the item do not properly load, and therefore do not reflect the preview that was shown to the user before she bought it.[676] As a consequence of the textures not loading, the user's virtual avatar cannot walk over the land or it falls through the hole caused by the lack of textures.

Given that there is no intention to defraud the buyer in this example, at first glance it may seem that she is not able to rescind the agreement because of the rule in *Seddon*.[677] However, Section 44 of the Sale of Goods and Supply of Services Act 1980 (SOGGSA) removes the rule in *Seddon* where a transaction concerns the sale of 'goods'.[678] This raises the question as to whether certain digital assets can constitute goods. Traditionally, only software supplied along with hardware could be considered goods. However, the European Court of Justice (ECJ) held in *The Software Incubator Ltd v Computer Associates (UK) Ltd* that goods are things that 'can

[675] Paul S Davies, 'RESCISSION FOR MISREPRESENTATION' (2016) 75 The Cambridge Law Journal 15.
[676] If this is a static NFT rather than a dynamic NFT, the buyer will be unable to edit the asset to fix the issue even if she had the technical knowledge to do so. Haya R Hasan and others, 'NFTs for Combating Deepfakes and Fake Metaverse Digital Contents' (2024) 25 Internet of Things 101133, 6.
[677] In other words, this is an example of an innocent misrepresentation. It is worth noting that the courts are stricter in rescinding a contract where a misrepresentation is innocent. *See* McDermott (n 193) [14.130].
[678] Sale of Goods and Supply of Services Act 1980, s 44.

be valued in money and which are capable, as such, of forming the subject of commercial transactions'.[679] Another requirement set out in the judgment provides that the software must be provided under a perpetual licence. Therefore, given that they are essentially a form of software, NFTs, cryptocurrencies and other digital assets may constitute goods for the purposes of SOGSSA.

Furthermore, the Consumer Rights Act 2022 in Ireland, which transposes Directive 2019/770/EU on Contracts for the Supply of Digital Content and Services (DCSD), clarifies the remedies available to consumers of digital goods.[680] The DCSD has provided clarification as to the rights and remedies available to consumers in relation to digital content purchases. Article 8(1) of the Directive is particularly relevant for the purposes of our defective Metaverse asset as it requires that digital content should be 'fit for the purposes for which comparable digital content would be used'.[681] Article 8(1)(b) further states that the digital content must have the functionality and compatibility which are assessed based on the 'nature of the goods'.[682] However, parties will only be able to rescind the agreement where the problem with the digital content is serious, or 'not minor'.[683] This caveat reflects the potential for trivial errors to be written into code, and therefore prevents the floodgates from opening for myriad claims against software developers. Yet, the problem set out in our hypothetical could be classified as a more serious issue as it is fundamental to the contract that the consumer can 'enjoy' the virtual land. The enjoyment of the land in this regard means that she should be able to view it as it was intended without a glitch-filled display, and that she should be able to traverse the land using her virtual avatar without falling into an 'endless void' caused by the

[679] C – 410/19 *The Software Incubator Ltd v Computer Associates (UK) Ltd* [2021] OJ 742/, para 34.
[680] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] *OJ* L136 (DCSD).
[681] DCSD, Art 8(1)(a).
[682] DCSD, Art 8(1)(b). The rules on conformity of digital goods are set out by Consumer Rights Act 2022, ss 17 and 18 respectively.
[683] DCSD, Art 14(6), transposed in Consumer Rights Act 2022, s 26 (3).

problematic computer code. The smart contract for the defective Metaverse item could therefore be rescinded, in theory. Only by recognising that the error in the digital asset sold under the contract is significant can the courts recognise the norm which would render the loss of the plaintiff as normative.[684] If the loss is normative, the courts have identified a reason to render the defendant liable as it has caused the loss to the plaintiff.

To be sure, the DCSD overcomes the challenges once posed by the rule in *Seddon* by recognising the prevalence of digital goods in the technological era. Bringing digital content within the scope of contract law in this way is essential because commerce will continue to be digitalised through the further development of blockchains and virtual reality, as well as the integration of these two technologies. Therefore, consumers will increasingly engage with digital goods as more products and services are rendered online. Even presently, digital goods like crypto tokens and NFTs are central to the digital economy.

However, the DCSD does not deal with the limitations of contract law remedies in response to blockchain based transactions specifically. This is because in practical terms, it is difficult to rescind a smart contract because its performance cannot be stopped once it has started because it is persistent in its automation of the written terms of the agreement.[685] Given that a contract must be rescinded prior to its execution, the smart contract's persistence in achieving its own full execution will prevent the agreement from being rescinded except for where there is fraud or if it is for the sale of goods. Therefore, the rules of rescission will have to be expanded if they are to encompass smart contract transactions more broadly. However, even if the rules are expanded, rescission may still be impracticable because of the technological obstacles that must be overcome.

[684] Weinrib, 'The Gains and Losses of Corrective Justice' (n 492) 287.
[685] Herian (n 192) 30.

Notably, the pseudonymity of parties in tandem with the immutability of smart contracts renders them difficult to rescind. On blockchains such as Ethereum and Bitcoin, it can be difficult to ascertain the identity of the contracting parties.[686] Notwithstanding that the smart contract in the earlier hypothetical should be rescinded because the user has purchased an item that is not fit for purpose, there are technical factors that inhibit such rescission. In particular, blockchains such as Ethereum render rescission difficult in practice.[687] This is due to the fact that smart contracting parties often use pseudonyms, and they are identifiable only be reference to an alphanumeric string of characters.[688] Without knowing the identity of the party who benefitted from the transaction, it will be difficult to unwind the smart contract once it has been executed. However, the parties may have known one another in the above hypothetical and the seller may willingly return the money paid for the faulty virtual asset subject to the contract's rescission. However, without knowledge of the counterparty's identity, unwinding the contract may be impossible. Under such circumstances, the parties cannot rescind the contract because to do so would require knowledge of the counterparty's identity so that a new smart contract can be created.

Even if the parties are identified, blockchains such as Ethereum are designed to prevent transactions from being unwound.[689] Of course, this is by design; blockchain technology deliberately prohibits the reversing of transactions so that parties can transact without having to trust one another. Part of this process involves ensuring that the transaction cannot be unilaterally undone. However, as a consequence, transactions cannot be reversed by anyone notwithstanding an order by the courts requiring rescission.

[686] Tatiana Cutts, 'Smart Contracts and Consumers' (2019) 122 West Virginia Law Review 389, 434.
[687] Olaf Meyer, 'Stopping the Unstoppable: Termination and Unwinding of Smart Contracts' (2020) 9 Journal of European Consumer and Market Law 17, 20
[688] ibid.
[689] Cieplak and Leefatt (n 396) 425.

As a result of the immutability of smart contracts, Marino and Juels argue that the courts' function as a remedial institute is obsolete and that rescission ought rather to be coded into the smart contract.[690] Rescission instead would take the form of a 'self-destruct' button that would effectively delete the code of the smart contract from the blockchain.[691] Typically, the immutability of the blockchain prevents the deletion of code from the record, but parties may now expressly code the ability to do so into their smart contract owing to developments in the blockchain in the interim since early scholarship on smart contracts. However, a self-destruct feature like that described by Marino and Juels is not a cure-all remedy and only effectively assists where both parties agree that the smart contract ought to be rescinded. The self-destruct feature in other words will be of little help in cases of misrepresentation, fraud, or unilateral mistake. Additionally, it would require that parties expressly include such a self-destruct feature in the smart contract's code. Although there is an incentive to do so (as it enables parties to abandon smart contracts that do not fulfil their intentions), many parties may not include such a function.[692] In that case, the parties will turn to the courts for a remedy who will then have to look beyond rescission where it may not be practicable to enforce.

6.4.2 Rescission in DASCs

There may be difficulty in identifying the grounds for rescinding a smart contract where it has the characteristics of a DASC. As the Court found in *Quoine Pte Ltd v B2C2 Ltd*, such smart contracts are largely deterministic and 'do and only do what they have been programmed to do'. [693] If this is the case, the courts may find that there is no need to rescind the smart contract

[690] Marino and Juels (n 663) 152.
[691] ibid 158.
[692] Andrew Luesley, 'Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada' (2019) 19 Asper Review of International Business and Trade Law 155, 168.
[693] *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 3, para 208.

– even if that smart contract performs in a manner that is contrary to the mutual will of the parties.

One example is the promotion of smart contracts which purportedly act as 'Maximal Extractable Value (MEV) bots' but are constituted by a malicious DASC. Used legitimately, an MEV bot executes trades to the benefit of its user by monitoring the data of a specified cryptocurrency on multiple exchanges.[694] However, malicious actors have misled users into deploying DASCs under the impression that the software would act as a crypto-asset trading bot. Instead of providing those users with a trading bot, the deployed smart contract would siphon the users' crypto-assets into the malicious actor's wallet. Provided that this interaction qualifies as fraud, the smart contract could be rescinded because the courts may try to restore the parties to a position as though the fraudulent statement had not been acted upon by the victim using rescission.[695] As a consequence of the perpetrator's use of misinformation, the victim's consent is not a 'genuine manifestation' of his 'self-determining agency'.[696]

In this context, the victim sought to obtain a crypto-asset trading bot. However, the wrongdoer manipulated him into deploying a DASC that is coded to deliver cryptocurrency to one or multiple crypto-wallet addresses belonging to the wrongdoer. If the DASC was not a genuine manifestation of the victim's self-determining agency, then it should be rescinded and the benefits of the transaction returned to him. The victim ultimately deployed the DASC, meaning that he was the *offeror*, and the wrongdoer simply accepted the offer. This means that the victim had an opportunity to inspect the code for himself. However, it was not apparent how the code

[694] 'Smart Contract Scams | Ethereum Drainers Pose as Trading Bots to Steal Crypto' (*SentinelOne*, 5 August 2025) <https://www.sentinelone.com/labs/smart-contract-scams-ethereum-drainers-pose-as-trading-bots-to-steal-crypto/> accessed 6 August 2025.
[695] *Northern Bank Finance v Charlton* [1979] IR 149, 197.
[696] Weinrib, 'Punishment and Disgorgement as Contract Remedies Symposium' (n 143) 89.

would function because the developer responsible for it used certain techniques to obfuscate the smart contract's true purpose.[697]

Notwithstanding the wrongdoer's apparent fraud, he may object to the rescission of the transaction because 'code is law', and to do so would upset the integrity of the blockchain. Under the 'code is law' idea, reversing a transaction is considered unfair even if the transaction itself was the result of unfairness (if not outright fraudulent).[698] If this is true, the DASC cannot be unstitched. However, one may identify the duty of the wrongdoer in the *YouTube* videos in which they promise to provide the victim with the trading bot. Rescission for fraudulent misrepresentation may therefore differ from rescission for mistake in a DASC. The reason is that there is some judicial support for the idea that 'code is law' where the vitiating factor is a mistake rather than a misrepresentation.

To be sure that a DASC formed under a mistake may not be rescinded, we can refer back to the case of *Quoine*.[699] To briefly recount the facts of the case, Quoine operated a cryptocurrency exchange and erroneously failed to make necessary changes to its Quoter Programme which was responsible for obtaining cryptocurrency market data. Consequently, Quoine's algorithmic trading programme sold Ether for Bitcoin at 250 times the market value. The Court held that the parties' automated contract could not be voided because it held there was no mistake involved. Low and Mik stated that the decision effectively constituted 'the development of what appears to be … a law of the horse, with the equine mammal standing in for

[697] 'Smart Contract Scams | Ethereum Drainers Pose as Trading Bots to Steal Crypto' (n 667): ['The attacker-controlled wallet address is obfuscated in each smart contract we analyzed and not directly visible in the smart contract code, which complicates identifying the weaponized contracts. We found multiple obfuscation techniques applied across different contracts to hide the attacker's [crypto-wallet]]'.
[698] Yeung (n 48) 234.
[699] *Quoine Pte Ltd v B2C2 Ltd* (n 216).

automation'.[700] It therefore seems that it may be difficult to rescind a DASC for a mistake, even where that mistake renders the parties' transaction unfair.[701]

However, agreements executed by code should be rescinded if those agreements should never have been formed in the first place. Specifically, a party should be granted a right to rescind the DASC where it 'lead[s] to a windfall to one party at the expense of the other', such as in *Quoine*.[702] Yet, the automated nature of the DASC in *Quoine* would seemingly bar the harmed party from seeking the remedy of rescission because it was difficult to determine the knowledge of the parties given that they had little involvement in the contracting process. However, rescission would provide corrective justice in such an instance, and should be obtainable in principle.

The reason is that DASCs are not formed in a vacuum, and the remedy of rescission would place the parties in a pre-contractual position. As Simon Thorley I.J. stated, DASCs like those used in *Quoine* 'have no mind of their own' and operate according to the instructions provided to them by their programmer.[703] The automation of the transaction is (or should be) inconsequential. The courts may instead adopt an 'honest and reasonable trader' test.[704] In so doing, the courts can identify where one party has made a windfall at the expense of the other. If the disparity exists, then corrective justice warrants a restoration of the status quo in the transaction because the transfer of the cryptocurrency was a consequence of a mistake. As such, the transfer was inconsistent with the appellant's rights and therefore, the cryptocurrency rightfully belongs to the appellant.[705] The remedy (in the form of rescission) may restore to the appellant that which rightfully belongs to it. However, the remedy only becomes available once

[700] Low and Mik (n 483) 2.
[701] For discussion of the *Quoine* case regarding the purported mistake and unfairness of the smart contract transaction, see Section 5.6.2.
[702] Luesley (n 665) 166.
[703] *B2C2 Ltd v Quoine Pte Ltd* (n 127).
[704] As proposed by Mance I.J. in his dissent. See *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA (I) 02 [198].
[705] Weinrib, *Corrective Justice* (n 8) 94.

the courts recognise the involvement of the human parties in forming the DASC, and avoid over-deference to the code's output.

6.4.3 Rescission of DAO smart contracts

Corrective justice centres on the rectification of a wrong by restoring parties to the state they occupied before the occurrence of the wrongful event. As a legal remedy, rescission embodies this principle by rendering the contract void *ab initio* and effectively unstitching the resulting transaction, thereby reinstating the status quo of the parties' interaction.

However, in the context of DAO smart contracts, this principle is presented with a challenge. Unlike bilateral smart contracts which have been negotiated and performed by identifiable parties, DAO smart contracts function autonomously on decentralised blockchains. The interactions facilitated by DAO smart contracts tend to involve multiple actors, such as the DAO's original investors, subsequent token holders, service providers, and others who extend beyond the original contracting parties.

When a DAO smart contract is rescinded to correct a wrongful act like that which occurred in the *DAO hack*, the aim of the remedy is corrective. It restores the parties' holdings and undoes the injustice resulting from the exploit because the transaction was contrary to the DAO's purposiveness. The attacker argued that the transaction adhered to the rules set out in the smart contract, treating it as though he had exercised a right granted by the smart contract's coded terms.[706] However, the smart contract existed to enable existing participants to split from the main DAO, withdraw their investments, or to transfer tokens. It was not intended that a third

[706] 'The DAO: What Was the DAO Hack?' (*Gemini*) <https://www.gemini.com/cryptopedia/the-dao-hack-makerdao, https://www.gemini.com/cryptopedia/the-dao-hack-makerdao> accessed 20 January 2025.

party could withdraw more than their invested amount, let alone $50 million worth of cryptocurrency.

Therefore, the rescission of the smart contract may also entail the retrieval of assets from parties who had legitimately transacted with the DAO by interacting with the smart contract at some point within its history. To do so would however infringe their right to the asset as no wrong has occurred between them. Corrective justice connects right and remedy, yet no remedy is necessary between the innocent participants and the DAO. However, the transactions are so technologically intertwined in the smart contract that it may be difficult to discern them.

However, rescinding a DAO smart contract may prove difficult regardless of whether a party's right has been infringed. Submissions to the blockchain are immutable, therefore once a smart contract has been deployed on the blockchain, it cannot be manipulated and it will perform regardless of the actions taken by the parties.[707] But rescission is supposed to involve a 'giving back and taking back on both sides', neatly encapsulating the form of corrective justice.[708] While 'giving back and taking back' may be doable in a bilateral smart contract transaction where the parties may know each other, in a DAO context, this reciprocal action may be more difficult. This has led Marino and Juels to conclude that the courts may be less useful in providing the remedy of rescission, and that rescission must be coded into the smart contract itself.[709] But the courts are 'justice ensouled' and have a distinct role under corrective justice to provide a remedy that responds to the injustice.[710] There is no guarantee that the parties will code a 'right' to rescission in their smart contracts, particularly in a DAO where there are multiple smart contracts to consider.

[707] Adam Sanitt, 'Remedies for Smart Legal Contracts: Rectification and Rescission Reconsidered' in Barış Soyer (ed), *Damages, Recoveries and Remedies in Shipping Law* (Informa Law from Routledge 2023) 106.
[708] *Newbigging v Adam* (1886) 34 Ch D 582.
[709] Marino and Juels (n 663) 152.
[710] Weinrib, 'Corrective Justice in a Nutshell' (n 13) 350.

6.5 Rectification

Following the advent of smart contracts, there may follow a resurgence of rectification as a judicial remedy.[711] Should this resurgence occur, it may be attributed to the need for legal remedies to address discrepancies or inaccuracies that arise in the execution of automated agreements. The objective of rectification is to give effect to party intention, and the courts do not use it to rewrite the parties' bargains.[712] The courts achieve this objective by ordering amendments to the words contained in the agreement where they do not accurately record the parties' agreement.

More specifically, there are two ways in which the need for rectification arises as identified by Leggatt L.J. in *FSHC Group Holdings Ltd v GLAS Trust Corporation Ltd*.[713] The first is where the parties form an agreement to execute a contract that contains particular terms, but they ultimately enter a contract with different terms. The second is where the parties do not make a prior agreement, but nonetheless there must be some common intention that exists between the parties which they expressed in some way, and that was not accurately recorded in the contract. *FSHC* has not been adopted by the courts in Ireland, but it provides a sound theoretical basis for an analysis of rectification. Nonetheless, the Irish position as summarised by McDermott does resemble that of *FSHC*.[714] First, there must exist a prior agreement concluded by the parties which the written contract was to render binding. Second, the written document must fail to register what was actually agreed upon by the parties. Third, it must fail to record the

[711] Green, 'Smart Contracts, Interpretation and Rectification' (n 160) 249.
[712] McKendrick, *Contract Law* (n 591) 198.
[713] *FSHC Group Holdings Ltd v GLAS Trust Corporation Ltd* [2019] EWCA Civ 1361.
[714] McDermott (n 193) [24.37].

common intention of the parties. Finally, it must be equitable to grant the remedy of rectification.

The remedy of rectification appears to have a role in providing corrective justice. In applying the remedy, the courts aim to ascertain 'what intention was communicated by one side to the other, and with what common intention and common agreement they made their bargain'.[715] In other words, the courts seek to determine the self-chosen purposes for which the parties contracted, and whether there was a failure to record those purposes.[716] If the parties' mutual purposes for the contract are not accurately captured, the courts may then rectify the agreement in writing.[717]

6.5.1 Bilateral smart contract rectification

Rectification may better provide corrective justice in the bilateral smart contract context. For example, rectification may be used in response to a smart contract for the sale of an NFT by one party to another. The purpose of the smart contract is to execute the transaction and manage the user's ownership over the asset. The asset in question may be an item in a video game for which the NFT authenticates the party's ownership over the asset.[718] Using NFTs, the holder of a digital asset may own rather than simply license the asset from the video game's publisher. Paul offers to sell a coveted in-game sword to Tom for €10,000 worth of cryptocurrency.[719]

---

[715] *Lovell & Christmas v Wall* (1911) 104 LT 85, 93.
[716] Weinrib, *Corrective Justice* (n 8) 114.
[717] *Irish Life Assurance v Dublin Land Securities Ltd* [1989] IR 253, 260.
[718] Fairfield argues that the tokenisation of in-game assets are a suitable use-case of NFTs. See Fairfield (n 362) 1266 ['Digital item sales called microtransactions already drive the videogame economy, from the sale of hats in games like 'Team Fortress' or 'Among Us' to the purchase of special vehicles, weapons, and armor in first-person shooters or massively multiplayer virtual worlds. Permitting gamers to truly own and resell what they buy or earn from the game creates a new incentive structure for hardcore players, who may be able to earn a living playing their favorite game.'].
[719] For the avoidance of doubt, people are willing to buy digital and in-game assets for significant sums of money. For example, an in-game sniper for the game 'CounterStrike: Global Offensive' was purchased for approximately $61,000. See Andy Chalk, 'CS:GO "Dragon Lore" AWP Skin Sells for More than $61,000' *PC Gamer* (31

Given that the parties know each other, and the value of the transaction, they decide to formalise the agreement in writing. The smart contract is used to exchange the NFT from Paul to Tom. The exchange involves the transferral of Paul's cryptocurrency to Tom's wallet and the NFT of the sword from Tom's holdings to those of Paul. However due to an error, the wrong item is identified in the code and Paul receives a 'common' item of a much lesser value.

Paul and Tom had effectively laboured under a common mistake, therefore it may be correct to rectify their agreement. The test for *common mistake* rectification was set out in *Daventry District Council v Daventry & District Housing Ltd.*[720] The test is satisfied if:

> (1) the parties had a common continuing intention, whether or not amounting to an agreement, in respect of a particular matter in the instrument to be rectified; (2) which existed at the time of execution of the instrument sought to be rectified; (3) such common continuing intention to be established objectively, that is to say by reference to what an objective observer would have thought the intentions of the parties to be; and (4) by mistake, the instrument did not reflect that common intention.[721]

The hypothetical satisfies the test because the common continuing intention and agreement of the parties was that Paul would receive the rare item instead of the common one. This is what they believed would occur at the time the agreement was executed by way of the smart contract. Objectively, it may be apparent that the parties had intended to exchange a rare item for €10,000 worth of cryptocurrency because this is expressly written in the natural language agreement *and* the item which Paul ultimately received was worth significantly less than the rare one for

January 2018) <https://www.pcgamer.com/csgo-dragon-lore-awp-skin-sells-for-more-than-61000/> accessed 21 March 2024.

[720] *Daventry District Council v Daventry & District Housing Ltd* (2012) 1 WLR 1333.

[721] ibid 80.

which the parties had bargained.[722] Finally, the instrument did not reflect the common intention of the parties because they both had in mind a self-determined purpose which was not manifested by the smart contract. Corrective justice requires that the contract is an expression of the self-determined purpose which was the subject of the parties' mutual assent.

As evidenced by the hypothetical above, the bilateral smart contract involves an extra step that is not typical of conventional contracting. The natural language agreement sets out what the parties agree upon and the smart contract subsequently self-enforces the agreement. The court's analysis of the bilateral smart contract may involve comparing the natural language document (the 'prior *legally enforceable* agreement') with the smart contract's code to determine how the agreement should be rectified.[723] Specifically, it may focus on the accuracy with which the parties' actual agreement had been translated into code format.[724]

The Irish Supreme Court in *Irish Life Assurance v Dublin Land Securities Ltd* provides clarity as to what is required before the courts may rectify an agreement.[725] Based on the criteria set out therein, the courts may be permitted to rectify an agreement like that in the hypothetical discussed above. First, there must be an agreement which precedes the instrument that the parties seek to rectify. This criterion is satisfied because the parties have created a natural language agreement. It is the smart contract's code which they will seek to rectify.[726]

Second, their agreement need not be in writing, but it may be beneficial in discharging the heavy burden of proof. The third (and related) criterion states that it is not required that the

[722] Davies argued that it is inappropriate to use the objective approach in common mistake rectification instead of referring to the parties' subjective intentions because 'it is artificial to insist that a common mistake exists simply by ignoring the true subjective intentions and looking at a prior objective accord'. See Paul S Davies, 'Rectifying the Course of Rectification' (2012) 75 Modern Law Review 412, 424; However, the courts should not be bound to investigate the parties' subjective intentions because these are opaque imaginings. Instead, the courts should examine the outward conduct of the parties which has an 'externally recognizable nature' upon which the courts can base their judgment. See Weinrib, *The Idea of Private Law* (n 18) 177.
[723] Green, 'Smart Contracts, Interpretation and Rectification' (n 160) 250.
[724] ibid 249.
[725] *Irish Life Assurance v Dublin Land Securities Ltd* (n 690).
[726] Herian (n 192) 27.

parties have concluded a contract so long as the parties were agreed on a term of an intended agreement. There must have been some outward expression and communication between the parties regarding the purported term.[727] Not all smart contracts will have an antecedent natural language agreement, however the existence of this document in Paul and Tom's case will benefit them for the purpose of ascertaining their agreement.[728] Moreover, given that the expression of the term need not be in the form of a contract, it may be sufficient that the parties have communicated over messaging applications such as WhatsApp or Discord as to their agreement regarding the sale of the virtual sword.

Consequently, Tom would be unable to claim that the parties had agreed to exchange the 'common' item as opposed to the rare sword. It is evident in the parties communication through the natural language agreement that the rare item was the subject matter of the bilateral smart contract but the code failed to reflect that. Corrective justice identifies Tom's receipt of Paul's cryptocurrency as a normative gain, and Paul's receipt of an item he did not desire as a normative loss. By rectifying the code, the courts can ensure that equality is restored to the parties by ensuring that Paul receives the asset to which he is entitled.[729] As Green notes however, the process for rectifying the smart contract's code even where there is a 'wet agreement' (a natural language agreement) is akin to the remedy of specific performance.[730] This is appropriate if it restores the equality of the parties' positions.

[727] *Irish Life Assurance v Dublin Land Securities Ltd* (n 690).
[728] Filatova argues that smart contracts without natural agreements are uncommon in practice. See Filatova (n 19) 234.
[729] Weinrib, *Idea* (n 14) 117.
[730] Green, 'Smart Contracts, Interpretation and Rectification' (n 160) 249.

6.5.2 Rectification of DASC transactions

The remedy of rectification exists to correct defects in the recording of the parties' agreement. Based on this definition of rectification, it may be difficult to rectify DASCs because this remedy is concerned with defects 'not in the making, but in the recording, of a contract.'[731] Difficulty therefore arises as DASCs are 'made' and 'recorded' at the same time and there are no prior discussions in which the parties form an agreement. For example, the smart contract in *Quoine* was formed spontaneously as a result of the two parties' respective algorithms communicating with one another. As such, the parties may not know the terms of the resulting contract before it had been concluded.[732] The parties are placed at arm's length from the contract formation process.

DASCs may therefore be incompatible with the doctrine of rectification set out in both *Daventry District Council* and *Irish Life Assurance*.[733] *Daventry* requires that the parties have a 'common continuing intention' with regard to the code of the smart contract that is due to be rectified. However, that 'intention' has been effectively outsourced to the parties' respective algorithms, therefore it is difficult to ascertain precisely what they intended by entering into the trades. Although the parties' intentions are 'manifested by' the instructions they provide to their algorithmic trading software and they may '*not want to know* about each and every transaction', there may be instances where corrective justice warrants a closer examination of the parties' intentions.[734] By analysing their intentions, the courts may identify the parties' self-

[731] McKendrick, *Contract Law* (n 591) 199.
[732] Damian P Cassar, 'The Notion of Mistake in Blockchain-Based Smart Contracts: An Analysis of B2C2 Ltd v Quoine Pte Ltd from a Comparative Perspective' (2023) 10 European Journal of Comparative Law and Governance 253, 268.
[733] *Daventry District Council v Daventry & District Housing Ltd* (n 693); *Irish Life Assurance v Dublin Land Securities Ltd* (n 690).
[734] On the manifestation of intention through contracting computer software, see Mik, 'The Resilience of Contract Law in Light of Technological Change' (n 224) 120.

determined purposes for entering the agreement in the first place. However, this may be difficult to do where the parties have deferred their capacity to self-determine to computer code.

Another obstacle to the rectification of a DASC is found in the criteria of *Irish Life Assurance*. Specifically, the first criterion which stipulates that the parties must have an agreement which precedes the instrument they wish to rectify. However, in a DASC, such an agreement does not exist because the smart contract 'is' purportedly the contract. Certain parameters are provided to the smart contract through its code, and it produces an output according to those constraints specified by the parties. At no stage did the parties state in a natural language that 'the desired trade will involve an exchange of 0.04 BTC for 1 ETH' or similar.

In effect, the agreement in a DASC is both 'made' and 'recorded' at the same time. The agreement does not come into being until the parties' respective algorithms form a unified interaction by mutually assenting to one another's terms. Prior to this moment, the parties cannot know what the terms of the agreement will be. And it is only when the algorithms connect in this way that the final contract is 'recorded' as the code is finalised according to the parties' inputted parameters.

Therefore, if rectification is concerned with the recording (rather than the making) of the contract's terms, then DASCs are potentially problematic when it comes to smart contract rectification.[735] Due to the courts' role in rectifying a contract by focusing on how it was recorded, it is unlikely that a DASC may be rectified. This is due primarily to the fact that the making and recording of the agreement occur simultaneously. In contrast, a bilateral smart contract with a preceding natural language document provides the courts a basis upon which to rectify the smart contract's code.

[735] See footnote 731.

DASCs therefore entail an unfortunate consequence for corrective justice where the rectification of the agreement is concerned. Fundamentally, the reason for this is the lack of an outward expression of the parties' accord. Although, it may be argued that the instructions which the parties provide to the computer prior to the contract's execution may constitute an expression of their accord.[736] However, the black-box nature of the DASC means that one party may not see those instructions, and therefore may not know even remotely the terms of the contract prior to its conclusion.[737] Consequently, it may be difficult to rectify the smart contract's code due to the lack of any initial accord of the parties. As a result, the corrective injustice arising out of the transaction may stand unless other remedies can be applied to restore the transactional imbalance resulting from the parties' interaction.

6.5.3 DAO smart contract rectification

Through the remedy of rectification, the courts may correct a contract by identifying a mistake that is common to both parties and renders the agreement as such that it does not manifest their purposiveness. However, the architecture of the blockchain may inhibit the rectification of smart contracts.[738] The complexity of DAO smart contracts exacerbate the effect of the blockchain's immutability. Once data is on the blockchain, it cannot be changed. This technical design may hinder the remedy of rectification as the courts will not be able to amend, or require that parties amend, a smart contract as easily as they could a conventional contract. The contract's original code will permanently exist on the blockchain after its deployment, including the errors contained within it.

[736] Sanitt (n 680) 105.
[737] Scholz (n 104) 152: ['Black box algorithmic contracts present a different type of problem than form contracts. Where those who accept form contracts can be said to be 'rationally ignorant,' in black box algorithmic contracts there is no fixed set of things of to which a party can be said to be ignorant. What the algorithm is going to do is unknown to both parties.'].
[738] Herian (n 192) 28.

Rectifying a traditional contract is relatively straightforward; a prior agreement between the parties is identified and the written document is corrected to better reflect the agreement to which the parties had actually manifested their consent. However, DAOs are different because they involve a multiplicity of interconnected smart contracts that operate autonomously and simultaneously to govern transactions upon the DAO. Because of this interconnectivity, correction may not simply entail changing a single line of code of one smart contract. In this way, the DAO smart contract differs from bilateral smart contracts and even DASCs because the courts may have to factor in all other contracts that constitute the DAO. The other smart contracts on the DAO must be carefully coordinated so that they align with the parties' intended purpose. Yet, the blockchain's immutability may prevent such the rectification of even one of those smart contracts.

For example, a majority of a DAO's participants may authorise a fee to external developers to undertake the maintenance of the organisation's architecture for 1 Bitcoin. The amount has been agreed upon also with the developers themselves. But due to an error in the code, the developers receive 2 Bitcoin. The transaction is processed through a number of smart contracts which authenticate the exchange of the stipulated value of Bitcoin. To bring the smart contract in line with the parties' manifested purposes, all the smart contracts responsible for governing the smart contract would also require rectification.

Moreover, rectification may not unfairly prejudice third parties, therefore if third parties have obtained any rights according to the agreement, the courts may not grant rectification.[739] Therefore, if the developers were also going to work on an external protocol which was necessary for the functioning of the DAO but is nevertheless a separate entity, the courts may decline to rectify the parties' agreement. Consequently, the DAO's participants may have to

[739] Davies (n 722) 422; McDermott (n 193) para 24.37.

cope with the loss sustained under the smart contract notwithstanding that the loss was normative. This shows the problem of the interconnectedness of coded smart contracts within DAOs and how it may prevent the parties from rectifying the agreement to better reflect the terms to which they actually agreed.

6.6 Injunctions

Injunctions are equitable remedies, and the courts have discretion as to whether they should be granted. This discretion is demonstrated when the courts decide the remedy that is most appropriate based on the facts of the case; particularly the question posed is whether it is fairer to award damages or an injunction.[740] This exercise of reasoning we have seen already in *Osbourne v Persons Unknown*, in which an injunction was favoured because the involved NFTs were of personal value to the claimant.[741]

However, scholars like Goldberg and Zipursky argue that injunctive remedies undermine corrective justice because such measures are forward-looking to a time before a wrong has occurred.[742] However, corrective justice permits the use of injunctions because it is concerned with the 'structure of the injustice and the consequent structure of the remedy'.[743] The distance in time between the remedy and the wrong does not factor into the equation. Consequently, corrective justice justifies the use of an injunction where it prevents the doer of harm from continuing to inflict that harm on the sufferer.[744]

[740] *O'Neill v Ryan (No 3)* [1992] 1 IR 166 at 196 (per Finlay C.J.).
[741] *Lavinia Deborah Osbourne v Persons Unknown* [2022] EWHC 1021 (Comm).
[742] Andrew S Gold, 'A Moral Rights Theory of Private Law' (2010) 52 William and Mary Law Review 1873, 1892.
[743] Weinrib, 'Civil Recourse and Corrective Justice' (n 658) 287.
[744] ibid.

Initially, injunctions appear to be the most suitable remedy available to the courts for crypto-related cases. This is because smart contracts and blockchains render it difficult to determine damages. It is therefore more practicable to prevent the parties from taking a certain course of action or insist that they take a specific course of action as a means to return the harmed party to the position they were in prior to the transaction. However, preventative injunctions are only one step in this process while legal proceedings are ongoing. Nonetheless, it is an important step because the misappropriated assets can otherwise be dispersed via a web of smart contracts and concealed behind various crypto-wallet numbers. Mareva injunctions and preservation orders are useful in this regard as they can stall parties who have misappropriated assets from dissipating them further.

Before the courts will grant a prohibitory injunction, the plaintiff must satisfy the test set out by Lord Diplock in *American Cyanamid v Ethicon Ltd*.[745] This test was applied in one of the key English cases concerning crypto-assets, *AA v Persons* Unknown.[746] In that case, the unknown defendants obtained Bitcoin from a Canadian insurance company by blackmailing them. The first criterion of the test requires that there is a serious question to be tried.

6.6.1 A serious issue about smart contracts?

When the plaintiff argues that there is a serious question to be tried, she does not have to prove to the courts that she will be successful in obtaining a final injunction. Instead, she must demonstrate that the claim is neither frivolous nor vexatious.[747] In addressing this part of the test in *AA v Persons Unknown*, the Court stated that it was satisfied there was a serious issue to be tried in relation to two of the four defendants because they participated in the extortion and ransom of the claimants.[748] Additionally, in *Fetch.ai v Persons Unknown*, the Court was

[745] *American Cyanamid v Ethicon Ltd* [1975] AC 396.
[746] *AA v Persons Unknown* [2020] 4 WLR 35, 12.
[747] *American Cyanamid v Ethicon Ltd* [1975] AC 396, 407G.
[748] *AA v Persons Unknown* [2020] 4 WLR 35, 12.

also satisfied that there was a serious issue to be tried where the defendants accessed the claimant's account and moved its cryptocurrencies to third-party accounts.[749] Therefore, a serious issue to be tried may be identified in some cases concerning smart contracts and crypto-asset transactions.

6.6.2 Bilateral smart contract injunctions

Smart contracts may be used to transfer the ownership title over real estate. In practice, the smart contract would automatically exchange cryptocurrency for the title.[750] Given that real estate transactions may involve the exchange of significant sums of money, the parties would *ideally* set out their correlative rights and duties in a natural language document.

A contract for the exchange of real estate in this manner should be clearly explained between the parties so that the parties understand their rights and duties. An injunction may be required where the terms of the contract are not upheld by the parties. For example, a smart contract may be used for the sale of tokens representing ownership over a luxury apartment block in County Dublin. Using the smart contract, Grace purchases a 10% stake in the apartments. As part of the written terms of the agreement, she agrees not to sell her stake within the first three months. However, after one month has passed, she identifies a better investment opportunity elsewhere and sells her stake. In so doing, she breached her agreement with the developers.

One possible solution for the developers would have been to code the three-month restriction into the smart contract that governs the token. This way, Grace could not have sold her token earlier than permitted under the agreement. As they failed to do this however, the next step would be to seek an injunction because Grace has broken a promise that she would not sell the

[749] *Fetch.ai v Persons Unknown* [2021] EWHC 2254 (Comm), para 16.
[750] Filatova (n 19) 223.

token until a specified time. The goal of the injunction would be to prevent the sale of the token. The courts are traditionally open to enforcing negative covenants such as the one in this scenario even where the loss can be calculated in monetary terms.[751] However, it may be impossible to halt the sale at this point. The issue here is that smart contracts are autonomous, self-executing and immutable.[752] Therefore, if Grace's smart contract was executed, the transaction is immutably recorded on the blockchain and cannot be stopped by notice from the courts or the party seeking the injunction. Giancaspro is correct in stating that the enforcement of injunctions in relation to smart contracts may be 'far more complex' than their application to conventional contracts.[753] However, it is not impossible to enforce an injunction simply because it is applicable to a smart contract transaction.

6.6.3 Injunctions in the DASC context

Although harmed parties have been successful in obtaining interlocutory injunctions to freeze the assets *in situ* while the courts figure out the substantive legal questions, there are reasons to be concerned about the role of injunctions going forward. The purpose of the injunction is to restore to the plaintiff 'the thing of which [he] was wrongfully deprived.'[754] In the DASC context, the plaintiff is typically deprived of a crypto-asset such as a form of cryptocurrency or an NFT.

AA v Persons Unknown has fast become the classic example in English law where an injunction was issued in a crypto asset case.[755] In that case, a hacker purportedly infected the computer system of the plaintiff, a Canadian insurance company, and infected it with malware. The

[751] McDermott (n 193) [22.04]; *Dublin Port and Docks Board v Britannia Dredging Co Ltd* [1968] IR 136.
[752] Giancaspro, 'Is a "Smart Contract" Really a Smart Idea?' (n 216) 832.
[753] ibid.
[754] Weinrib, *Corrective Justice* (n 8) 112 Emphasis added.
[755] *AA v Persons Unknown* (n 94).

hacker subsequently sent ransom notes to the company's customers, assuring that those who paid would receive a decryption tool to unlock their computer. A particular customer paid the ransom of 109.25 Bitcoin – the equivalent of $950,000 at the time.[756] The Bitcoin would likely have been transferred from the victim to the hacker using a smart contract. The plaintiff sought to recover the lost Bitcoin by way of injunction.

Corrective justice may be instantiated by the award of an injunction in this case. Through its blackmail, the attacker made a wrongful gain by extorting the victim in return for the decryption tool. Although not a contractual right, the victim had a right to enjoy the Bitcoin which it had obtained, and the hacker had a correlative duty not to infringe upon that right. Although the Bitcoin was sent using a smart contract, the right to the Bitcoin may not be transferred because the smart contract was the result of the attacker's blackmail. Therefore, in taking the victim's Bitcoin in this way, the hacker had interfered with the plaintiff's enjoyment of its own property.[757]

An injunction was granted based on established principles, rendering the Bitcoin recoverable by the plaintiff.[758] Therefore, even without an explicit contractual arrangement between the parties, the courts may identify the infringement of the plaintiff's rights which necessitates the rebalancing of the parties' holdings. Injunctions are therefore a useful remedy for crypto-asset transactions and may address injustices even in DASC contexts where the rights and duties are not expressly set out by the parties.

An injunction was also granted in the case of *D'Aloia v Persons Unknown*, although the Court did so without express reference to *AA*.[759] Specifically, the Court granted an interim freezing

[756] In August 2025 at the time of writing, Bitcoin had a conversion rate of 1 BTC = $112,758, meaning that the ransom if executed today would equal $12,299,593.88.
[757] Weinrib, *Corrective Justice* (n 8) 112.
[758] Condon (n 115) 226.
[759] *D'Aloia v Persons Unknown* [2022] EWHC 1723 (Ch).

injunction with respect to misappropriated crypto-assets. The plaintiff in that case claimed that the unknown defendants fraudulently misappropriated a significant sum of his cryptocurrencies; 2.1 million USDT and 230,000 USDC. Persons unknown used a website with the domain name 'www.tda-finan.com' to deceive users to believe that it is linked to TD Ameritrade, a legitimate renowned brokerage. The deceptive tactics included the use of a logo bearing resemblance to that of TD Ameritrade.[760] As a consequence of the defendant's deception, the plaintiff transferred the cryptocurrencies from two of his crypto wallets operated by Coinbase and Crypto.com respectively. Trower J. found that there was a serious issue to be tried because there was a 'relatively straightforward claim in deceit'.[761] Moreover, he found that that damages were an inadequate remedy because the cryptocurrencies still belonged to the plaintiff, and damages would not prevent the defendant from disposing of those assets.[762]

Due to the background risk of persons unknown disposing of the crypto-asset before the courts can assess the case with regard to the substantive legal issues involved, injunctions may ensure that the plaintiff's right can still be vindicated. Unlike other remedies discussed in this chapter, injunctions may be applied more readily both to bilateral smart contracts and DASCs, as demonstrated by *AA v Persons Unknown* and *D'Aloia v Persons Unknown*.[763] The reason is that although a DASC does not contain any express contractual rights and duties, the plaintiff has a proprietary interest over the cryptocurrency which the defendant has a duty to not infringe. The cryptocurrency's owner has the right to determine how that cryptocurrency is to be used which places a correlative duty on the defendant to not use or sell it.[764] Although Weinrib argues for gain-based damages where a defendant uses the plaintiff's property, an injunction is more appropriate in the context of digital assets where they may be rapidly

[760] ibid 2.
[761] ibid 34.
[762] ibid 28–29.
[763] *AA v Persons Unknown* (n 94); *D'Aloia v Persons Unknown* (n 732).
[764] Weinrib, *Corrective Justice* (n 8) 125–126.

dissipated through various crypto wallets and rendered unrecoverable by the plaintiff. As he also argues, injunctive relief may instantiate corrective justice by preventing the defendant from continuing the wrong into the future.[765] The courts may prevent the continuation of the wrong into the future by ensuring the defendant does not conceal the asset by passing it through multiple crypto wallets, and ultimately selling it to realise a profit.

6.6.4 Injunctions against DAOs

Injunctions have proved useful in preventing the continuation of wrongdoing into the future in the bilateral smart contract and DASC contexts. As such, they are a useful way of ensuring corrective justice in some blockchain-based transactions because they see that the plaintiff's right may be vindicated.[766] The effect of an injunction in a peer-to-peer transaction is to prevent certain actions or transactions which may be brought about by the creation of a new smart contract. In a DAO however, each smart contract acts as a cog in the machine that keeps the organisation going. All of its operations are encoded and automated using these smart contracts. Once the smart contract is entered into the DAO's infrastructure, it may be difficult to halt parties from interacting with that smart contract in order to gain from it. DAO smart contracts stand in contrast to bilateral smart contracts and DASCs which tend to depend on fewer other smart contracts and also consist of simpler code.

Instead with DAOs, the courts may only ascertain whether an injunction is permissible by examining all the other smart contracts which constitute the organisation. Only by doing so may they determine whether the defendant has acted in a way that warrants an injunction. Once the courts identify a sufferer and a doer within a particular action on the DAO, an injunction

[765] Weinrib, 'Civil Recourse and Corrective Justice' (n 658) 287.
[766] ibid 289.

may be granted to prevent the defendant from acting in a way that is contrary to the purposes of the DAO. For instance, the injunction may be used to stop the unknown attackers in the *DAO hack* from further disbursing the withdrawn cryptocurrencies, and to return them to the DAO. If the injunction achieves this, it may effectively restore the parties to a position as though the harm had not occurred.

Injunctions may even be useful where the DAO is the doer of the wrong rather than the sufferer. For example, a DAO may be created to manage a decentralised investment fund using smart contracts that autonomously execute investments and distribute profits to token holders. Subsequently, the DAO (through an amendment of the smart contract) begins making high-risk investments that expose the fund to significant losses, despite assurances that the investments would be low to medium risk only. This means that, when the investors entered the DAO, the DAO undertook a duty only to make investments of a particular risk profile. This correlates with the investors' right where performance takes the shape of those types of investments only. The courts may maintain the parties' equal freedom by ensuring that the DAO's performance of its duty aligns with the performance right of the investors.[767] The injunction is a suitable means for doing so as it would halt the DAO from making risky investments that were contrary to the investors' right. Therefore, it appears that injunctions may instantiate corrective justice across the three smart contract taxonomies.

6.7 Terminating the smart contract

6.7.1 Bilateral smart contract termination

An innocent party may elect to terminate a contract if a condition contained in the contract has been breached. However, termination is a 'self-help' remedy as the courts are not required to

[767] Weinrib, *Reciprocal Freedom* (n 33) 33.

declare that a contract has been terminated. Instead, the party who breached the contract may challenge the non-breaching party's termination, and this the extent of the courts' role in the remedy of termination.[768] To terminate the contract, one party is required to show clearly to the other party that they are treating the contract as at an end. A case in point is *Vitol SA v Norelf Ltd, The Santa Clara*, in which Norelf agreed to sell propane to Vitol.[769] Vitol repudiated the contract via telex on the belief that the cargo would not arrive on time. The reason for this belief was that the propane was due to be shipped before 7 March but it was still being loaded on 8 March. The ship finally sailed by 9 March notwithstanding Vitol's attempted repudiation of the contract. Norelf subsequently sued Vitol for breach of contract and sought damages. However, an arbitrator found that Vitol's telex constituted an anticipatory breach, which Norelf accepted by not taking any further steps to perform the contract. The courts' role was to confirm whether the non-breaching party was entitled to terminate the contract (or in this case, whether the arbitrator was correct in its holding that termination was permitted).

The termination of contract remedy may figure in corrective justice theory in the following way. The parties set out with a common, self-determined purpose for which they enter into a contract. Under the contract, the plaintiff obtains a right to the defendant's performance, correlative to which the defendant obtains a duty to perform. Drawing on *Vitol*, a right was established under the contract which entitled Vitol to the delivery of the propane, under which Norelf had a duty to carry out the same. By repudiating the contract, Vitol had effectively discharged Norelf of its duty to perform, and correlatively, Vitol's right to performance ceases to exist. This was contingent on Norelf's acceptance of the repudiation, and thus the termination of the contract. Vitol's repudiation is evidence of its self-determining agency to bring to an end a contract which no longer serves its purposes (i.e. that the cargo would no longer arrive on

[768] Mindy Chen-Wishart, *Contract Law* (Oxford University Press 2012) 462.
[769] *Vitol SA v Norelf Ltd, The Santa Clara* [1996] AC 800.

time). Norelf signalled its acceptance of the repudiation by no longer pursuing the object of the contract.

Where a bilateral smart contract is concerned, termination may unfold in a manner similar to *Vitol*. A buyer may enter into a contract with a seller for a digital asset like a batch of tokenised commodities. In the natural language agreement, the parties agree to a deadline of 3 August by which the seller must transfer the tokens to the buyer. However, the commodities were not tokenised in sufficient time and the seller sends a message to the buyer to indicate that the token batch will not be prepared for transfer until a later date. As such, the buyer repudiates the contract as constituted by the natural language document because it no longer serves his purposes. As a consequence, the seller does not follow up on the interaction, indicating that he has terminated the agreement.

The termination in this hypothetical is possible because the interaction is in the form of a bilateral smart contract. The smart contract has not yet been posted or executed, therefore the termination of the agreement is much like termination in a conventional contract. The buyer has indicated in advance of the contract's performance (which would have been facilitated by the smart contract) that he intends to repudiate the contract. As such, the parties can reciprocally bring to an end their rights and duties because the contract no longer aligns with their purposiveness.

6.7.2 Repudiation and termination of a DASC

Terminating a DASC differs from the termination of a bilateral smart contract because of its characteristics. DASCs are those agreements that are expressed entirely in the form of computer code. The code may be finalised by the offeror, a developer working on behalf of the offeror, or an algorithm (such as in *B2C2 v Quoine*). Termination of a fully coded agreement is

either unnecessary because the smart contract prevents repudiation, or not possible because the right of the non-breaching party to terminate the agreement may not be apparent in the contract's code. I will turn to these issues below.

The first issue is that a smart contract without a natural language agreement cannot be repudiated and therefore termination by the non-breaching party is unnecessary. A breach of contract constitutes a repudiation if the breach goes to the root of the contract.[770] The test for repudiation seeks to determine whether the breach deprives the non-breaching party of substantially the whole benefit of the contract as expressed within the contract.[771] As such, the courts are required by the test to identify what constitutes the whole benefit of the contract.

However, identifying the whole benefit of the contract may be difficult if it is expressed entirely in the form of computer code. The reason is that language is central to determining whether a contract has been repudiated so as to justify its termination by the other party. As the Court in *Decro-Wall International v Practitioners in Marketing* stated, the legal consequences of a contractual breach is determined by looking to the contract's terms.[772] As such, if there is no term in the contract expressly or impliedly to suggest that the contract should be repudiated, then the courts may not be satisfied that it should have been repudiated in the first place. The question which Diplock L.J. posed in *Hong Kong Fir Shipping v Kawasaki Kisen Kaisha Ltd* was whether 'the occurrence of the event deprive[d] the party who ha[d] further undertakings still to perform of substantially the whole benefit which it was the intention of the parties as expressed in the contract…'.[773] As such, the courts may only find that the defendant had the right to terminate a given contract if they understand what the contract says. However, deciphering the terms of the smart contract may be difficult without the guidance of a natural

[770] *Decro-Wall International v Practitioners in Marketing* [1971] 1 WLR 361, 368.
[771] *Hong Kong Fir Shipping Co Ltd v Kawasaki Kisen Kaisha Ltd* [1962] 2 QB 26, 69.
[772] *Decro-Wall International v Practitioners in Marketing* (n 743).
[773] *Hong Kong Fir Shipping Co Ltd v Kawasaki Kisen Kaisha Ltd* (n 744).

language document. A human party's comprehension of computer code and its outcome may be limited until after it has executed and fully performed its code. Consequently, determining the main benefit of the smart contract may be a fruitless exercise.

Another area where the termination of a DASC may fail is related to the parties' inability to see the other parties' conduct. Unlike in bilateral smart contracts, it may be difficult for the non-breaching party to claim that the smart contract should be terminated. The reason is that the courts are required to look at the repudiating party's conduct to determine whether he clearly refuses to perform the contract.[774] The conduct or intention of a party to a DASC to perform may not be apparent to the non-breaching party because of the anonymity of the parties. However, the parties to a DASC may not refuse to perform in the same way they might in a bilateral smart contract. The reason is that a smart contract may not refuse to perform after the point at which it has been deployed on the blockchain.[775] Therefore, repudiation, and termination, of a DASC may be difficult and unnecessary in some circumstances.

On the one hand, the DASC holds parties to their bargains by ensuring that they cannot back out once the smart contract is submitted to the blockchain. The Weinribian account of contract law (through its adoption of Kantian right) centres on the entitlement of the offeree to the performance of the offeror. Ordinarily, where the offeror fails to perform according to the offeree's entitlement, thus breaching the contract, this constitutes a wrong to the offeree under the corrective justice framework.[776] However, given that a DASC may not go unperformed by the offeror who has posted it to the blockchain, our concern is not that the smart contract may be repudiated (and consequently terminated). Instead, the nature of the smart contract is such

[774] *Mersey Steel and Iron Co v Naylor Benzon & Co* (1884) 9 App Cas 434, 438–439.
[775] Mik, 'Smart Contracts' (n 2) 280; Green, 'Smart Contracts, Interpretation and Rectification' (n 160) 251.
[776] Weinrib, 'Punishment and Disgorgement as Contract Remedies Symposium' (n 143) 75.

that it cannot be stopped even if the offeror wishes to repudiate it. As such, the opportunity for termination for repudiation may not arise.

6.7.3 Termination of a DAO smart contract

DAOs are governed entirely by code, which means that all rules and actions including the terms of parties' interactions are accounted for in the code of the smart contracts that constitute the DAOs structure. If there is an interparty dispute that warrants the termination of one of the DAO's smart contracts, it may be difficult to restore parties to their pre-contractual positions unless the DAO has provided in the code for such termination. The reason is that the smart contract will continue to perform notwithstanding any decision by the parties or the courts to terminate the agreement.[777] Ordinarily, termination occurs before the contract is performed but this may be difficult for the parties to do in a DAO context because there are multiple smart contracts, few of which the parties may predict their outcome. Given the interconnected nature of these contracts, termination of one smart contract may have a ripple effect on the others within the nexus.

For example, a DAO may be created for disbursing research grants using autonomous smart contracts for voting, treasury management, and project milestones. One major participant, 'ProjectY', undertakes to deliver key research milestones and receive grant payments through the DAO's smart contract system. Halfway through the project, ProjectY states in an on-chain message that it will not complete the agreed milestones, expressing that it intends to repudiate the smart contract through which it received its funding. The other DAO participants, noting the repudiation, may seek to have the smart contract terminated. The normative loss and correlative gain of the parties will continue to increase. The correlative gain in this instance is constituted by ProjectY's receipt of funds without providing the corresponding value, and the

[777] Marino and Juels (n 663) 153.

loss is the DAO's missed milestones and potentially wasted resources. From a corrective justice standpoint, the contracts to be terminated are those which pay ProjectY, and those which set out the relevant milestones and deadlines. However, to fully correct the imbalance in the parties' holdings may involve the termination of multiple smart contracts that do not exclusively relate immediately to the doer and sufferer of the repudiatory breach. Consequently, termination may have effects on third parties within the DAO. This is because the termination of all relevant smart contracts to achieve complete restoration to the parties' status quo ante may also impact participants seeking grants unrelated to ProjectY, or those who are involved in milestone review and may not be paid for their assistance because of the smart contracts' termination.

6.8 Conclusion

While smart contracts in many scenarios will ensure performance and prevent breach or vitiation, this thesis has argued that there may be instances where the parties will turn to the courts to seek a remedy. Particularly, where a party's actions conducted by way of smart contract are inconsistent with the parties' equal freedom, then a remedy must follow the injustice.[778] Particularly, the courts may be required to provide a remedy where the defendant's actions infringe the performance right of the plaintiff. The purpose of the remedy then is to vindicate the plaintiff's right by providing him with what is rightfully his.[779] However, there are both considerations of principle and practice that may prevent the courts from doing so. Where the mechanisms of the transaction are complex, undoing the consequences of the transaction may prove difficult, and thus the courts may struggle to vindicate the plaintiff's right. Where the parties' agreement is expressed first in plain language and then in code, the

[778] Weinrib, *Corrective Justice* (n 8) 36.
[779] ibid 93.

courts may at least ascertain the right to be remediated. And if the parties have communicated in such a way, there is a possibility that they will be identifiable to one another and a remedy may be more readily applied to their interaction. However, where the agreement is decentralised and autonomous in its nature, and where the code performs the transaction deterministically, a remedy may not follow any harm that arises so easily. For one reason, identifying the wrong to be remedied may be more difficult because the code is the only source of the parties' agreement. Another reason is that the smart contract may have executed immutably and the transaction cannot be easily unstitched without engaging the other party. The DAO smart contract exaggerates the features of a DASC, thereby rendering it even more difficult in certain circumstances to provide a remedy. By involving a multiplicity of smart contracts, many of which are only expressed in code, the target of the remedy may be less apparent. It appears that injunctions provide the semblance of corrective justice through our three smart contract taxonomies by preventing the continuation of the defendant's wrong, although they still apply with some difficulty.

7 Unjust Enrichment: A Response for the Non-Contractual DASCs and DAOs

7.1 Introduction

The preceding chapters have analysed smart contracts using the law of contract from a corrective justice purview. It was found early on in this thesis that DASCs and DAO smart contracts may not be mapped onto the doctrines of contract formation. The reason for this is that they are not a manifestation of the parties' self-determination. A contract – and therefore a smart contract – is supposed to represent the parties' purposiveness, meaning that both parties enter into the contract with a particular end in mind. However, a code-only agreement may contradict their purposiveness. The purpose begins as an idea in the minds of the contracting parties which is then realised by the parties through their agreement.[780] Yet, by outsourcing their capacity for self-determination to the smart contract's code, the purpose that was conceived in the parties' minds may not materialise as they had expected. Where the code determines the terms of the agreement, the concluded 'contract' may not represent their will at all. Moreover, where the terms of the agreement are available for inspection by the offeree in their code-form, these may be too abstract to be properly comprehended by him. Under corrective justice, the parties' relationship is structured in a bipolar manner, demonstrated particularly by the process of offer-and-acceptance in the contract law context.[781] This bipolarity may not exist where the offer is unintelligible to its reader (in a way that computer code is to many of us), such that the offeree's acceptance of it may be defective. If this is true, then the smart contract is not a contract, however the transaction will still be completed once consideration is submitted by the offeree, notwithstanding his

[780] Ernest J Weinrib, *The Idea of Private Law* (Oxford University Press 2012) 89.
[781] ibid 74.

inability to understand its terms. Therefore, the courts may still be required to assess the transaction if the plaintiff argues that he has sustained a normative loss.

Without a remedy in contract, the plaintiff may instead turn to the law of unjust enrichment which exists within contract law's 'shadow'.[782] In particular, the law of unjust enrichment permits the plaintiff to reverse a transfer of value that was the result of a mistake or fraud.[783] The factor of mistake or fraud evinces the plaintiff's lack of intention to provide the defendant with anything of value, and therefore an obligation arises requiring the defendant to return the benefit to the plaintiff.[784] Although this thesis was concerned with contract law and the smart contract, it is necessary as a final step to identify a means of recovery in transactions involving DASCs and DAOs. By referring to the *Quoine* case and other extra-legal scenarios addressed throughout this thesis, the chapter explains how immutable smart contracts in code-only form accentuates the possibility for mistake. Where there is a lack of a legal contract between the parties, the required nexus may be created by the defendant's acceptance of the transfer as non-gratuitously provided by the plaintiff, coupled with the plaintiff's lack of intention. *Quoine* and the 'Cryptopunk' scenario serve as two examples here where the transferee likely lacked the intention for the transfer because the DASC's code performed in a manner that did not expect. The upshot of the unjust enrichment approach is further explained by reference to *D'Aloia v Persons Unknown*. Finally, the chapter draws upon the example of the so-called 'DAO hack' where unjust enrichment may be used as by the DAO's participants to recover their losses resulting from the 'attackers' exploitation of a vulnerability contained in the DAO's smart contract.

[782] Jared I Mayer, 'Unjust Enrichment and the Unwritten Law of Corporate Reorganizations' (2023) 23 UC Davis Business Law Journal 181, 189.
[783] *Dargamo Holdings Ltd v Avonwick Holdings Ltd* [2021] EWCA Civ 1149, at [58].
[784] Ernest J Weinrib, *Corrective Justice* (Oxford University Press 2012) 204.

7.2 Principles of unjust enrichment

Unjust enrichment is situated in the shadow of contract. Where the parties set out the terms of their interaction in a contract, the law of contract governs the transaction and the recovery is not possible through unjust enrichment. If the plaintiff was permitted to recover using unjust enrichment where there is a contract in place, the effect would be to undermine the parties' agreement.[785] However, contract law's reach is limited where the wrong takes place through an interaction that does not involve a bargain between the parties.[786] In this context, the law of unjust enrichment takes point for the purpose of determining whether there is any reason for holding the defendant liable. Fundamentally, the law of unjust enrichment requires the return of money or property to the plaintiff where it would be unjust for the defendant to retain it.[787] There are four elements to unjust enrichment that must be satisfied before the courts will order the defendant to return the benefit to the plaintiff.[788]

The first criterion states that the defendant must have been enriched, meaning that he must have received a benefit from the plaintiff. However, the question as to the defendant's enrichment goes largely unaddressed by the courts because his receipt of a benefit in the form of money or other property is usually self-evident.[789] Once this benefit has been transferred from the plaintiff's holdings to the defendant's holdings, enrichment has occurred. For example, a transfer of value that increases the defendant's holdings or improves his position may constitute his enrichment.

---

[785] Eli Ball, *Enrichment and the Claimant's Expense: Attribution Rules in Unjust Enrichment* (Bloomsbury Publishing 2016) 183.
[786] Jared I Mayer, 'Unjust Enrichment and the Unwritten Law of Corporate Reorganizations' (2023) 23 UC Davis Business Law Journal 181, 189.
[787] *Corporation of Dublin v Building and Allied Trade Union* [1996] 1 IR 468, 483.
[788] *Bank of Cyprus UK Ltd v Menelaou* [2015] UKSC 6, [2016] AC 176, para 18.
[789] Peter Birks, *Unjust Enrichment* (Oxford University Press 2003) 43.

The second requirement is that the enrichment must have occurred at the plaintiff's expense. A claim in unjust enrichment may not be sustained unless the plaintiff has suffered the loss of something for which she did not receive something of comparable value in return. This requirement ensures that only the specific plaintiff and defendant are linked for the purposes of liability.[790] If the parties are not directly connected by the plaintiff's diminished holdings, then liability would be too expansive if it was imposed by the courts on the parties.[791] Only a plaintiff who has suffered a loss in this manner may claim for unjust enrichment, thus limiting the prospect of broader claims by non-involved parties.

The third criterion states that the defendant's enrichment must have been unjust. An enrichment is rendered unjust where the transferor lacked the intention to transfer the value to the recipient. Where this intention is present, the transferor may not recover the value because the transfer may be considered just.[792] Therefore before the courts may permit the transferor to recover the value, they must find a basis upon which they may find that the transferee's enrichment was unjust. Generally, such unjustness is identified where the value was transferred as a result of a mistaken payment. The fact that the payment was 'mistaken' itself provides a reason to reverse the transfer because it signifies the transferor's lack of intention, and consequently, the unjustness of the enrichment.[793]

Fundamentally, the elements of unjust enrichment embody corrective justice. Although the transfer does not involve the blameworthiness of the defendant, the enrichment is unjust it is unjust because it is normatively defective. For instance, the defendant did not infringe a

[790] Ernest J Weinrib, 'Correctively Unjust Enrichment' in Robert Chambers, Charles Mitchell and James Penner (eds), *Philosophical Foundations of the Law of Unjust Enrichment* (Oxford University Press 2009) 37.
[791] ibid.
[792] Ernest J Weinrib, *Corrective Justice* (Oxford University Press 2012) 202.
[793] Peter Birks, 'Unjust Enrichment and Wrongful Enrichment Symposium: Restitution and Unjust Enrichment' (2000) 79 Texas Law Review 1767, 1779–1780.

contractual right of the plaintiff or commit a tort.[794] But in receiving value which the plaintiff did not intend to provide, restitution restores both parties to a position as though the transfer did not occur – thus correcting the defective transfer.[795] Taken together, the features of unjust enrichment exhibit the elements of corrective justice.

The features of corrective justice are set out in Chapter 2, and it is unnecessary to revisit them in detail at this point. To recall briefly, corrective justice requires that the plaintiff and defendant are bipolarly situated, that the plaintiff has a right to which the defendant has a correlative duty, and that both parties interact as free and equal agents.

When it comes to unjust enrichment, the existence of a plaintiff and defendant nexus is apparent. The typical unjust enrichment case involves a plaintiff who claims that the defendant was enriched at his expense. However, difficulty purportedly arises in relation to the second requirement concerning the correlative right and duty of the parties. The reason is that the manner in which the defendant is enriched, on its face, does not obligate her to return the benefit of the transfer. Given that she passively received the value of the transfer, it may not be clear that she breached a duty that she owed to the plaintiff. In this regard, the defendant is 'blameless'.[796] The law applies equally to both parties, meaning that the courts may not refer to the plaintiff's lack of intention in isolation to determine the defendant's duty.[797] To ensure this equality is present in their determination, the law of unjust enrichment draws on the absence of the plaintiff's intention *as well as* the defendant's acceptance of the benefit that was not provided for free.[798] Once these two conditions are satisfied, the defendant incurs an obligation to return the benefit of the transfer to the plaintiff.

---

[794] Dennis Klimchuk, 'Unjust Enrichment and Corrective Justice' in Jason W Neyers, Mitchell McInnes and Stephen GA Pitel (eds), *Understanding Unjust Enrichment* (Bloomsbury Publishing 2004) 134.
[795] *Kingstreet Investments v. New Brunswick (Department of Finance)* [2007] 1 SCR 3, [32], quoted in Weinrib, *Corrective Justice* (n 8), 187.
[796] Klimchuk (n 794) 134.
[797] Weinrib, 'Correctively Unjust Enrichment' (n 790) 41.
[798] ibid 42.

7.3 Unjust enrichment and DASCs

Contract law may fail to provide corrective justice if it is unable to rectify the liability between two parties where the plaintiff has incurred a normative loss and the defendant has obtained a normative gain. The risk of this failure is more probable where the smart contract is expressed entirely in the form of computer code. For these types of smart contract, the courts may instead turn to the law of unjust enrichment which exists within contract law's 'shadow'.[799] Instead, a claim in unjust enrichment may be sustained where a contract does not exist within a particular transaction, either because it is never formed, or because it is void or voidable. Where there is a 'normatively defective transfer of value' in the absence of a contract, liability for unjust enrichment may arise. As such, a DASC (which I argue lacks the status of an enforceable contract), may be subject to the law of unjust enrichment so that the pre-transactional equality of the parties may be restored. Our unjust enrichment analysis leaves off from our earlier conclusion that DASCs and DAO smart contracts are not contracts in the legal sense. They may be better understood as software-mediated interactions between parties for the exchange of value devoid of legal recognition under contract law.[800]

D'Aloia v Persons Unknown is one case involving a DASC in which the plaintiff claimed the defendant was unjustly enriched.[801] In that case, the plaintiff was induced to transfer an amount of the Tether cryptocurrency valued at approximately $2.5 million. That cryptocurrency was passed through various crypto-wallets before ultimately being withdrawn by the seventh defendants. However, the judgment in question did not address the seventh

[799] Jared I Mayer, 'Unjust Enrichment and the Unwritten Law of Corporate Reorganizations' (2023) 23 UC Davis Business Law Journal 181, 189.
[800] For example, Gamper sees the smart contract 'as a way to coordinate actions without agreement'. See Florian Gamper, 'A Non-Contractual Approach to Smart Contracts' (2023) 31 International Journal of Law and Information Technology 231, 237.
[801] *D'Aloia v Persons Unknown* (2025) 1 WLR 821.

defendant directly and instead concerned the sixth defendant, a cryptocurrency exchange called Bitkub. The seventh defendants purportedly had accounts with Bitkub.

The plaintiff's case suffered from a fundamental flaw. There was no connection between him and the seventh defendant to render liability between them. Although the Court found that the Tether cryptocurrency constitutes a form of enrichment, the plaintiff did not show that the enrichment occurred at his expense because he failed to demonstrate that it entered Bitkub's crypto-wallet.[802] In effect, Bitkub was the incorrect defendant against whom to bring a claim as it was not proven that they accepted the non-gratuitous transfer of the Tether from D'Aloia.

However, the Court found that the transfer of the Tether from D'Aloia was unjust. In particular, D'Aloia claimed that the transfer was unjust because it was both an unauthorised payment and money paid under mistake.[803] The reason was that he made the transfers as a consequence of inducements made by the first defendants (Persons Unknown) who allegedly operated a scam using a website called 'td-finan'.[804] The Court was therefore satisfied that the transfer was unjust because D'Aloia was a victim of fraud.[805] He made the transfers only because of the fraudulent misrepresentations made by Persons Unknown.

The dispute in *D'Aloia* was a useful starting point for our unjust enrichment analysis. It shows how unjust factors may manifest in the realm of smart contracting. When the plaintiff only has access to website-based inducements and the smart contract's code, the ultimate outcome of the transaction may be contrary to his intentions. It is clear, however, that the plaintiff must identify the correct defendant for taking an unjust enrichment claim. As a factual matter, this may be difficult to establish in cases like *D'Aloia* where the value is

[802] ibid 829–830.
[803] ibid 830.
[804] ibid 842.
[805] ibid 886.

transferred through multiple intermediaries. Here, it was Persons Unknown rather than Bitkub who was enriched *at the expense of the plaintiff*.

Another example of unjust enrichment may be found in *B2C2 Ltd v Quoine Pte Ltd*, although it was also found there that there was no unjust enrichment. [806] This chapter disagrees with the finding of the decision, the reasons for which are set out below. At the centre of that dispute was the transfer of Quoine's 3029 Bitcoin for B2C2's 309 Ether – a trade that was executed as 250 times the market rate.[807] The trades were a consequence of Quoine's coding error in its Quoter Programme. As well as arguing that there was a unilateral mistake, Quoine also claimed that B2C2 had been unjustly enriched. The SICC was satisfied that the first two criteria for a claim in unjust enrichment were established in this case, namely that B2C2 was enriched at the expense of Quoine.[808]

However, Quoine's argument failed on the third criterion because the Court found that the enrichment of B2C2 was not unjust. The reason for this conclusion was based on the purported existence of a contract between the two parties. The Court stated that claims of unjust enrichment may only succeed in exceptional circumstances in contexts where a valid contract exists, and that *B2C2* was not such a case.[809] The Singapore Court of Appeal elaborated that there could be no unjust enrichment because the contract between the parties was in place which effectively barred Quoine from bringing a claim based on unjust enrichment.[810] The existence of a contract proves the transaction is just because the transferee receives an *in personam* right to the performance of the contract. As such, he is entitled to

[806] *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC (I) 03.
[807] ibid, [4].
[808] ibid, [245].
[809] ibid, [252].
[810] *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA (I) 02, [135] - [136].

receive the benefit, an entitlement which offsets any concerns as to the justness of the transfer.

It was argued earlier in this chapter (and elsewhere in this thesis) that smart contracts constituted by code alone may not be contracts. As such, the recipient of the benefit does not obtain a right to receive the benefit from the transferor where such a smart contract is used. However, this alone would be insufficient as the non-existence of a contract itself does not indicate that the transaction was unjust. As set out in the previous section, there must be a concrete basis for determining that the transfer was unjust.

A transfer is just if it aligns with the mutual will of the transferor *and* the transferee.[811] A transfer will therefore be unjust where the transferor lacked the intention to provide the benefit in return for nothing or something of nominal value relative to the transferred benefit. And correlatively, the transferee must have accepted the benefit as a gift that the transferor did not intend to provide. In such circumstances, there is no reciprocation between the parties for the transfer, and therefore, it does not correspond to their wills.

There is, therefore, a basis for finding liability in *Quoine* because the transfer of value was unjust, thereby satisfying the third criterion for unjust enrichment. Mance I.J. draws upon his own judgment in *Cressman v Coys of Kensington*,[812] and argues that there are parallels between it and *Quoine*. In *Cressman*, a purchaser incidentally obtained a valuable registration plate because it was attached to the vehicle he bought from the vendor. There was no contract for the transfer of the plate, the provision of which was a mistake by the vendor. Mance I.J. found that the transferee's enrichment was unjust notwithstanding his contention that he was blameless and that the plate was merely attached to the car which he purchased. The reason

[811] Ernest J Weinrib, 'The Corrective Justice of Liability for Unjust Enrichment' in Elise Bant, Kit Barker and Simone Degeling (eds), *Research Handbook on Unjust Enrichment and Restitution* (Edward Elgar Publishing 2020) 174.
[812] *Cressman v Coys of Kensington* [2004] EWCA Civ 47.

for this finding was that the transferee had not bargained for or paid for the plate, indicating that the transfer was carried out mistakenly.[813] In identifying the commonality between *Cressman* and *Quoine*, Mance I.J. stated that a failure to return a benefit that was erroneously transferred was unjustified.[814] And it was evident that B2C2 knew that Quoine had mistakenly transferred its cryptocurrency because the former sent an email titled 'Major Quoine database breakdown' to the latter.[815] In such circumstances, it would be unjust to permit B2C2 to retain the cryptocurrency it had acquired through the erroneous trades. The trade ought to conform to the will of Quoine as the transferor, which it did not.[816] It is more likely that Quoine's will was to trade the assets at a value closer to the going market rate at the time of the error as it was the objective of its Quoter Programme to obtain the market prices of the traded assets. Moreover, B2C2's email indicates that it accepted the transfer despite knowing that it was made by Quoine without donative intent.[817] This renders the liability connection between both parties, and therefore I argue, that B2C2 had been unjustly enriched.

The unjust enrichment analysis not only explains the issue at the centre of *Quoine*, but also illuminates liability in other instances of smart contracting. The sale of the NFT, CryptoPunk #2386, is one example where the law of unjust enrichment may justify the removal of the asset from the buyer and returned to the seller. To briefly recall the facts of that situation, the CryptoPunk was for sale via Niftex, and online NFT marketplace which had become defunct in the interim. Because the frontend website was no longer available, the buyer instead identified the DASC situated in the backend of the website.[818] The DASC remained

[813] ibid [37].
[814] *Quoine Pte Ltd v B2C2 Ltd* (n 810), [205].
[815] ibid, [203].
[816] Weinrib, 'The Corrective Justice of Liability for Unjust Enrichment' (n 811) 178.
[817] ibid 177.
[818] Molly White, 'CryptoPunk Sells for a Fraction of Its Likely Market Price Due to Zombie Smart Contract' (*Web3 is Going Just Great*, 11 September 2024) <https://web3isgoinggreat.com/single/cryptopunk-niftex-sale> accessed 9 December 2025.

executable due to its immutability once deployed on the blockchain, notwithstanding that the marketplace platform had ceased to exist.

Those who propose that 'code is law' may argue that the performance of the smart contract in the CryptoPunk scenario should stand. After all, the sellers were content to sell the asset and coded the smart contract as such. They may therefore argue that the transfer was just as it was facilitated by a valid contract (in its code-only form). However, the sellers were mostly unaware that a buyer had placed a counter-offer that significantly undercut the value of the asset. During the time when the marketplace was online, the website would have notified the sellers of the asset that a prospective buyer has made such a counter-offer. However, due to the marketplace's non-existence, the notification system was no longer available to the sellers. This highlights the perils of the 'code is law' approach specifically in the smart contracting context.[819]

The CryptoPunk transfer may be rectified through the law of unjust enrichment because the code did not reflect the parties' mutual will. The facts satisfy the criteria for liability in unjust enrichment. The transferee was enriched as the recipient of the NFT. His enrichment was at the expense of the transferors who had been stripped of an asset valued at 600 Ether (worth approximately $1.5 million at the time).[820] And finally, the transfer may be unjust because the holders of the NFT likely lacked the intention for two reasons. First, they may not have known that the asset was still available to buy considering the marketplace upon which it was hosted was offline. And second, they may not have transferred it for the low price of $23,000

[819] Although I am critical of the 'code is law' thesis in the smart contracting context, using code to form the architecture of cyber-spaces is generally useful. In recent times for example, large language models have been used to alter images against the will of the original uploader of the image. Code permits, but can also restrict, one's ability to edit such images using artificial intelligence. However, in the smart contract context, code may perform in a manner contrary to the parties' mutual will in which case private law may intervene to rectify the liability.

[820] Instead, they received $23,000. See Jason Nelson, 'CryptoPunks NFT Worth $1.5 Million Just Sold for $23,000—Here's How' (*Decrypt*, 12 September 2024) <https://decrypt.co/249012/cryptopunks-nft-worth-1-5-million-sold-23000> accessed 16 September 2024.

considering the price at which it was valued. Moreover, given the circumstances, the transferee accepted the transfer which he may have known was unintended by the transferors. This knowledge derives from the fact that he had to access the DASC through the website's backend, therefore knowing that the transferors would not be notified about the counter-offer.

7.4 Unjust enrichment and DAO smart contracts

Unjust enrichment may also provide a means to rectify the liabilities that arise in the context of the DAO. It was argued throughout the thesis that it may be difficult to establish the existence of a contract in a DAO, or how such a contract (if it exists) may be vitiated. There may, however, be a basis for restitution where one party becomes unjustly enriched through the execution of a DAO-based smart contract.

To illustrate this point, 'The DAO hack' is one example where unjust enrichment may provide an avenue for recovery for those users who have suffered significant losses. To briefly recall the facts of that scenario, 'The DAO' was established on the blockchain as a decentralised venture capital organisation. Its purpose was to invest in blockchain-based projects using the funds pooled together by its investors. However, one of the smart contracts within the DAO's infrastructure contained a vulnerability which permitted those funds to be siphoned by a user from the DAO's treasury into their own cryptocurrency wallet. 'Code is king purists' argued against the reversal of the cryptocurrency transfer notwithstanding the means by which the transferee procured it.[821] However, the majority favoured a software-based solution in the form of 'hard fork', thereby creating a new version of the Ethereum blockchain and partially recovering the withdrawn assets.[822] Had this event culminated in a

[821] Alexandros A Papantoniou, 'Smart Contracts in the New Era of Contract Law' (2020) 1 Digital Law Journal 8, 19.
[822] Wouter Dammers, 'How to Govern King Code' in Liisa Albertha Wilhelmina Janssens (ed), *The Art of Ethics in the Information Society: Mind You* (Amsterdam University Press 2016) 37.

legal dispute, the affected participants of the DAO may argue that the transferee had been unjustly enriched.

In terms of the first criterion for unjust enrichment, it is evident that the individual who siphoned off the funds had been enriched. The enrichment took the form of the $60 million worth of Ether that entered the transferee's crypto wallet.

The second question then is whether the enrichment was at the expense of any potential plaintiff. This criterion involves some complexity in relation to DAOs because they are unincorporated associations which may not sue or be sued under their own name.[823] Consequently, the DAO itself may not be the plaintiff at whose expense the enrichment was made, and the plaintiffs may instead include the transferors to which the cryptocurrency rightfully belonged prior to the transfer. As the DAO was non-custodial, the participants retained control over their invested assets, meaning the loss of those assets was directly at their expense. The transfer was at the participants' expense because they may not access the cryptocurrency which they had previously purchased using fiat currency. In essence, the exploit was akin to an ATM withdrawal *if* the ATM permitted the user to take out more money than they had available in their own account.[824] By doing so, the user would eventually start taking money that does not belong to them (i.e. the bank's money). By way of analogy, the individual who exercised the exploit on the DAO withdrew funds from the investors' pooled cryptocurrency.

Furthermore, the exploit satisfies the third criterion for unjust enrichment because the withdrawal of the cryptocurrency was unjust. However, some members of the broader blockchain community resisted claims that the transfer was unjust because of the purported

[823] For discussion of the legal character of DAOs, see Section 3.7.6.
[824] The ATM analogy was made by Morrison, Mazey, and Wingreen. See Robbie Morrison, Natasha CHL Mazey and Stephen C Wingreen, 'The DAO Controversy: The Case for a New Species of Corporate Governance?' (2020) 3 Frontiers in Blockchain 1, 6.

'fundamental principle of smart contracting' that coded contracts are to be upheld based on the principle of *pacta sunt servanda*.[825] Notwithstanding the adherence by some of the community to this principle, is good reason for finding that the transfers were unjust. First, as argued earlier and throughout this thesis, such 'contracts' are not contracts in the legal sense. Had an enforceable contract existed, then the law of unjust enrichment would not be applicable to this scenario (and to DAOs more broadly).[826] However, without a clear expression of the DAO's participants' intention to transfer $60 million worth of Ether to the transferee, then there is no right of performance established, nor do the participants obtain a duty to provide the Ether to the individual who identified the exploit. As such, the community may not rely on the principle of *pacta sunt servanda*. The participants' will for that Ether was for investing in blockchain-based projects. And by 'accepting' the smart contract, knowing that the participants had other plans for the pooled funds, a duty is established on the transferee to return the cryptocurrency they siphoned into their own crypto wallet.

By turning to the law of unjust enrichment instead of contract law, the transferees may overcome the obstacles which contract law faces in its response to DAO smart contracts. Although the smart contract may not set out the parties' correlative rights and duties, unjust enrichment may be identified in absence of a contract where the transferee is at fault. Such fault arises where there is a normatively defective transfer of value, the existence of which generates an *in personam* right for the plaintiff, and a corresponding duty to return the value on the defendant.[827] By holding on to the cryptocurrency withdrawn from the DAO despite its participants' lack of intention for the transfer, the transferees obtain a duty to return the cryptocurrency to those from whom it was taken.

[825] Adam J Kolber, 'Not-So-Smart Blockchain Contracts and Artificial Responsibility' (2018) 21 Stanford Technology Law Review 198, 202; Dammers (n 280) 37.
[826] *Quoine Pte Ltd v B2C2 Ltd* (n 810), [135].
[827] Weinrib, *Corrective Justice* (n 792) 227.

7.5 Conclusion

The law of unjust enrichment provides an avenue for recovery for plaintiffs who suffer loss through DASCs and DAOs. This chapter identified the theoretical and doctrinal bases for finding unjust enrichment in smart contract transactions. From a theoretical perspective, corrective justice requires that the defendant returns any asset to the plaintiff that was received as part of a normatively defective transfer. A transfer is defective if it takes place in the absence of the plaintiff's intention, coupled with the defendant's acceptance of the transferred asset as not having been provided for nothing. By retaining the asset, liability arises and the defendant is required to provide the asset back to the plaintiff because the transfer executed contrary to the parties' mutual will.[828] These conditions are doctrinally expressed in the form of the three criteria which state that the defendant ought to have been enriched, at the expense of the plaintiff, and that the enrichment was unjust. The fact of the enrichment and its correlative effect on the plaintiff bipolarly links the two parties for the purposes of liability. The requirement that the transaction be unjust refers the parties' wills, the fundamental question being whether the parties mutually intended for the transfer or if it was the consequence of a mistake.

The complexity of computer code increases the likelihood of unjust transfers of digital assets. In the absence of a contract, the plaintiff in a case involving a DASC or DAO may instead turn to the law of unjust enrichment. This chapter drew upon real-world examples of crypto-asset transfers which it argued were unjust. First, the *Quoine* case showed that algorithms may produce results that no reasonable trader would consider in designing the code for their trading systems. It is unjust where the defendant knows that the smart contract executed in a

[828] ibid.

manner that was blatantly mistaken and accepts it as such. This knowledge was demonstrated by the email sent by B2C2 to Quoine. Second, the scenario of the 'CryptoPunk' NFT, where the transferee identified a DASC in the backend of a defunct online marketplace. This was unjust because the transferors had no notice of the transferee's attempt to execute the DASC, and it was not apparent that they intended to sell the asset anymore. Finally, the 'DAO hack' wherein the transferee executed a smart contract which contained a vulnerability, and siphoning the participants' funds into his own crypto-wallet. The inclusion of the vulnerability was not a deliberate act by the DAO, a fact which the transferee knew and accepted. In all these instances, unjust enrichment (and not contract law) may provide the transferor with an avenue for recovering their lost assets. However, these events merely scratch the surface of smart contract related losses, and such losses will continue to arise due to the unreliable nature of computer coded transactions. By identifying and applying the principles of unjust enrichment to such interactions, this chapter has provided harmed parties with a roadmap to recovering their crypto-assets.

8 Conclusion

This thesis examined the fit of the smart contract with contract law's doctrines through a corrective justice framework. The framework drew upon Weinrib's theory of private law as corrective justice because it provided a 'pure theory' of contract through which the smart contract could be analysed. As a pure theory, it enabled the analysis of the smart contract strictly as a transactional device with potential corrective injustice consequences. This meant that the examination would not be distracted by considerations of efficiency. This way, it remained steadfast in its effort to identify whether the smart contract is aligned with private law's kind, character, and unity, and whether it facilitates the juridical relationship and the correlativity that underpins it. To summarise the answer, the smart contract fits uneasily with contract law as understood through the corrective justice paradigm.

This conclusion contradicts the findings of some of the scholarship that came before it; most notably, the UK Law Commission's conclusion that existing legal principles may be adequately applied to smart contracts (although with slight developments in the law to account for specific contexts). From a theoretical and a doctrinal standpoint, contract law may not be neatly applied to smart contracts in certain circumstances so as to rectify the injustice between parties through liability.

The first point of issue is encountered in examining the applicability of the doctrines of formation to smart contracts. It is at the offer and acceptance stage of the contracting process that the offeree's entitlement to the offeror's performance is established in the fiat contract context. The offer and the correlative acceptance must be unequivocal, and the parties must be fully *ad idem* as to the terms of their interaction. The parties to a bilateral smart contract may reach mutual agreement more readily because the terms are displayed clearly in a natural language document. The smart contract's code merely animates those terms, thereby

satisfying the offeror's duty and the offeree's correlative right. However, where the offer is both express in, and performed by, the smart contract's code (such as in DASCs and DAO smart contracts), the ability of the offeree to comprehend the code is diminished. If the code is unintelligible to the offeree, then he cannot be bound by it because he cannot assent to that which he does not understand. The effect of the smart contract on the formative doctrines are particularly felt where the offeree has no opportunity to inspect the terms, such as in *B2C2 Ltd v Quoine Pte Ltd*. If the smart contract is simultaneously formed and executed, the resulting transaction may be contrary to the will of the offeree. As a result, no nexus is formed between the parties, and therefore no contract is established.

While DASCs and DAOs posed problems for doctrines of offer and acceptance, similar issues did not arise in relation to the doctrines of consideration and intention to create legal relations. A smart contract, no matter its form, requires the submission of some value (typically in the form of cryptocurrency). The amount of cryptocurrency is stipulated within the smart contract's code. This cryptocurrency serves as a token of the parties' willingness to engage as equal participants in the creation of the smart contract. For this reason, smart contracts, regardless of kind, pose no considerable challenges for the doctrine of consideration. Similarly, the doctrine of intention to create legal relations is unproblematic in our analysis because many smart contracts are created for commercial reasons rather than familial or social interactions. The courts will simply have to assess the purpose for the underlying transaction to determine whether the presumption of an intention to create legal relations stands.

The next point of analysis concerned the interpretation of smart contracts. From a corrective justice standpoint, the doctrine of interpretation is important because it objectively identifies the purposes for which the parties entered into the contract. To ascertain the parties' objective intentions, the courts need only look to the natural language document that forms part of the

bilateral smart contract. It is through this document that the will of the parties may be determined. However, in the DASC context where this document does not exist, the courts' analysis will turn on the smart contract's code alone. In this setting, interpretation will only help the courts understand the code and how it will execute rather than how it should execute according to the parties' mutual will. For this reason, the doctrine of interpretation does not enable the courts to intervene in the smart contract's execution even if it upsets the transactional equilibrium of the parties. The doctrine faces similar challenges in relation to DAO smart contracts, however the challenges in this context are exacerbated by the DAO's complexity. Because the DAO is constituted by a nexus of smart contracts, each smart contract may have to be interpreted in light of the others contained within the overall network of smart contracts that form the DAO. However, given that the DAO is often established for a particular purpose, the courts may at least take this into account when it interprets the smart contracts contained in its network.

Following the interpretation analysis, the next chapter focused on the vitiation of smart contracts. In a bilateral smart contract, vitiation may occur where there is a discrepancy between the natural language document and the performance of its terms through the smart contract's code. As the parties' correlative rights and duties are established in the natural language document, the computer code must accurately capture them in order to satisfy the offeree's performance right. Failure to do so may lead to the voidability of the contract for mistake or misrepresentation. From *Quoine*, it may be observed that the courts are reluctant to interfere with transactions that are formed and performed autonomously using computer code. However, the chapter found that Quoine had suffered a normative loss sufficient to ground its claim in mistake. By rejecting Quoine's argument that the transaction was the result of a mistake, the decision in that case does not conform to corrective justice.

With regard to misrepresentation, an actionable statement of fact may be written into a natural language document if it misrepresents the purpose of the smart contract. Such a misrepresentation may be innocent where the offeror unknowingly states that the asset exchanged under the smart contract is authentic when in reality it is a copy. A scenario like this may arise where the parties have entered into a contract offline, for example, through an auction sale. The courts may draw on the statements made regarding the asset to determine whether an innocent misrepresentation had been made, and if so, hold that the contract may be rescinded or award the offeree damages.

Furthermore, the creation of smart contracts has enabled a new form of fraud known as the 'rug-pull' where a crypto-asset is created and sold to investors with a view to withdraw its liquidity. The whitepaper or website used to promote these may include misrepresentations as the statements made within them do not correlate with the smart contract's code. Consequently, the rug-pull transaction does not involve the genuine consent of the offeree, and therefore liability would operate to rectify the injustice between the parties. The reason is that the offeree obtains a right to receive the crypto-asset as set out in the whitepaper or website. If these documents contain promises that the offeree will obtain access to other assets or that the token will increase in price, a misrepresentation may crystallise if it is evident the offeror never intended to provide these assets in the first place.

The final analysis within the chapter on vitiation concerned the frustration of smart contracts. It was highlighted in this chapter that smart contracts may be susceptible to frustration because of their digital nature. For this reason, they are vulnerable to cyberattacks, network outages, and glitches, which may render them incapable of being performed. Such eventualities are possible but may be unforeseeable. If the parties had expressed their respective rights and duties in a natural language document, their agreement may be frustrated if the smart contract cannot be executed or performed because its code is

inoperative due to technical difficulties. It was submitted that in such a scenario, the parties should be excused from performance of the terms of the natural language document. Even in the context where a DASC is used, the offeror may be relieved of any duty to perform the smart contract. In a bilateral smart contract, the parties may coordinate with one another to redo the transaction once the frustrating event has passed, or use a different blockchain that is not affected by the event. However, this may be difficult in the DASC context where the parties may not have any information about one another. Moreover, the original smart contract may continue to exist on the blockchain due to its immutability, pending execution once the network returns online.

The final 'contract law' chapter examines the remedies available under contract law, and the difficulties the courts may have applying these to smart contracts, both in practice and in principle. It found that breach of contract may occur in bilateral smart contracts where the offeror writes the smart contract's code in a manner that is contrary to the terms of the natural language agreement. If the parties opt to use a bilateral smart contract to order their affairs, the code must align with the pre-determined terms of the agreement, otherwise breach of contract may occur due to the late or non-performance of those terms. Given that the parties have a pre-existing relationship in the bilateral smart contract, and they are identifiable to one another and therefore the courts, damages may be the appropriate remedy because they remedy the losses inflicted by the defendant on the plaintiff. However, the same may not be true of the DASC which often involves parties who are anonymous to one another who may be trading assets which are incapable of being evaluated in monetary terms. Depending on the context, an NFT may be of sentimental value to the plaintiff and therefore the courts may decline to quantify it for the purposes of awarding damages.[829] In such cases, time is also of the essence because the misappropriated assets may be distributed to other crypto-wallets,

[829] Such as was the case in *Lavinia Deborah Osbourne v Persons Unknown* [2022] EWHC 1021 (Comm).

making it more difficult to trace them. For these reasons, the courts have opted to grant injunctions rather than damages where misappropriated crypto-assets were concerned.

The chapter then considered the implications of smart contracts for the remedy of specific performance. Specific performance ensures corrective justice by requiring the defendant to perform according to the duty he obtained from the contract. This remedy is particularly useful where the smart contract is used for the exchange of some novel asset. Cryptocurrencies exist in abundance and are therefore not sufficiently novel to require specific performance over damages. However an NFT is an asset that cannot be replicated and is unique to its recipient, and may therefore be subject to an order for specific performance. In a bilateral smart contract, specific performance will require the defendant to transfer the asset to the plaintiff in alignment with the terms agreed in the form of natural language. However, the remedy of specific performance encounters difficulties in the DASC context. Without a natural language agreement upon which to determine the parties' mutual will for the transaction. As such, an order for specific performance may merely enforce the same erroneous computer code that led to the parties' dispute in the first instance.

The next remedy considered by the chapter was that of rescission, which ensures corrective justice by setting the transaction aside. From a practical standpoint, rescission of all smart contracts may be difficult regardless of their form. Although parties are identifiable to one another in bilateral smart contracts, the immutability of the smart contract makes it practically difficult to reverse its effects. The only way in which a smart contract may be rescinded is if the parties have provided a mechanism for its reversal in its code. Without such a mechanism, rescission is not possible. However, the parties to a bilateral smart contract may, at least, create a new smart contract that will in effect reverse the transaction executed by the initial smart contract. They may do so because they have the benefit of knowing one another, and the reason for rescission may be based on the natural language agreement which the smart

contract purportedly performed. Where there is no natural language agreement, it may be difficult to unstitch a smart contract where it is difficult to prove that it was not a genuine manifestation of the parties' self-determination.

The chapter then analysed the remedy of rectification, which may have a resurgence in response to smart contracts because it is well-placed for correcting discrepancies that exist between a natural language agreement and a smart contract's code that does not accurately capture its terms. The courts' role will therefore involve examining the accuracy with which the parties had translated their agreement into the form of computer code. The natural language document is determinative of the parties' mutual will which the code may be corrected so that it performs according to its terms. The effect of rectification here is analogous to the remedy of specific performance. However, in the DASC context, rectification may not be applicable because its purpose is only to correct how the contract was recorded. It is not concerned with how the contract was formed. Consequently, where the contract is formed algorithmically and the parties are placed at arm's length from its creation, they may not know what the terms of their agreement will ultimately be. Due to the lack of any other outward expression of the parties' intentions, the courts may not rectify the recording of the transaction because there is no basis for them to do so.

The penultimate remedy examined by the chapter were injunctions. These legal devices ensure corrective justice by preventing the continuous infliction of harm by the defendant on the plaintiff. They are strong remedies for use in the smart contract context as the courts may identify an ongoing wrong perpetrated by the defendant and halt it by awarding an injunction. Their efficiency, in principle, was demonstrated across various crypto-asset related disputes including *Osbourne*, *AA v Persons Unknown*, and *D'Aloia v Persons Unknown*.[830] Although

[830] ibid; *AA v Persons Unknown* [2019] EWHC 3556 (Comm); *D'Aloia v Persons Unknown* [2022] EWHC 1723 (Ch).

in cases like *Osbourne*, there is infringement of a contractual right, the injunction nevertheless protects the proprietary interest that the plaintiff has in the misappropriated crypto-asset. Injunctions are an essential remedy because they prevent the further distribution of the crypto-assets taken from the plaintiff to other crypto-wallets, therefore making them hard to trace. The justification for the injunction here is that the defendant has a correlative duty not to use or sell the crypto-asset as this would be in conflict with the plaintiff's right over the asset.

The final remedy examined was that of termination. From a corrective justice perspective, termination by the non-breaching party extinguishes the parties' correlative right to, and duty of, performance under the contract. The chapter argued that the termination may arise in relation to bilateral smart contracts where the parties agree in natural language that a certain course of action will be taken by a particular date. Where the smart contract is not coded in sufficient time to execute the transaction by the date stipulated in the natural language document, the contract may be effectively repudiated. Consequently, the non-breaching party may be permitted terminate the smart contract. This is possible in the bilateral smart contract context where the smart contract for performing the agreement has not yet been deployed on the blockchain. However, there may be difficulty in determining that repudiation has occurred in a DASC because such repudiation is assessed according to the terms of the contract. In a DASC, where these terms are absent, identifying those terms may not be possible and as a consequence, the DASC may not be repudiated based on any particular terms. Moreover, although termination is possible based on the conduct of the party in breach of the contract, it may not possible to see the conduct that leads to the breach. As such, the conduct or intention of a party to a DASC may not provide an adequate basis upon which the non-breaching party may terminate the arrangement.

Ultimately, the thesis found that there are shortcomings in the doctrines and remedies available under contract law in their response to DASCs and DAOs. The law of unjust enrichment operates in the 'shadow' of contract law as a course of action when DASCs and DAOs fail to reflect the parties' mutual purposiveness or self-determination. Because code-only interactions may result in normatively defective transfers that contradict the parties' intentions, unjust enrichment ensures corrective justice by restoring the parties to their pre-contractual positions. This is possible, as the chapter argued that the three criteria of unjust enrichment may be satisfied in certain DASC and DAO contexts. The first criterion which requires that the transferee is enriched may be satisfied by receiving a benefit in the form of cryptocurrency or NFT. The second criterion is satisfied where the benefit was received at the expense of the transferor. A direct nexus between the transferor and the transferee is established once it is confirmed that the benefit was received at the expense of the transferor. This criterion may be satisfied by examining the specifics of the transfer as recorded on the blockchain. The record will show that the transferor's holdings have diminished while the transferee's have increased. The final requirement that the transfer is unjust is satisfied where the transferor lacks the intention to provide the benefit to the transferee. This lack of intention may be found in the form of mistaken transactions produced by the smart contract's code which no reasonable trader would make. As such, the law of unjust enrichment may serve to rectify smart contract losses resulting from erroneous code-enforced trades in cases like *Quoine*, the *DAO* hack, and the *CryptoPunk #2386* incident. It was argued that in these instances, the transferor's computer code had resulted in just transfers because the transferor lacked the intention to provide the benefit. This finding may apply more broadly to smart contract transactions, and ultimately, it is the law of unjust enrichment that may illuminate code-only agreements rather than the law of contract. Ultimately, identifying these

transactions as unjust allows the law to look past the literal execution of computer code to uphold the true will of the parties involved.

Bibliography

Case law

AA v Persons Unknown [2019] EWHC 3556 (Comm)

Albert v Motor Insurer's Bureau (1971) 2 All ER 1345

Associated Japanese Bank v Crédit du Nord (1989) 1 WLR 255

B2C2 Ltd v Quoine Pte Ltd [2019] SGHC (I) 03

Baird Textile Holdings Ltd v Marks & Spencer plc [2001] EWCA Civ 274

Balfour v Balfour (1919) 2 KB 571

Bank of Cyprus UK Ltd v Menelaou [2015] UKSC 6

Blue v Ashley [2017] EWHC 1928 (Comm)

Brodgen v Metropolitan Railway Company (1877) 2 AC 666

BS & N Ltd (BVI) v Micado Shipping Ltd (Malta) ('The Seaflower') (No 2) [2000] CLC 802

Cameron v Liverpool Victoria Insurance Co Ltd [2019] UKSC 6

Carlill v Carbolic Smoke Ball (1893) 1 QB 256

Chwee Kin Keong v Digilandmall.com Pte Ltd (2005) 1 SLR(R) 502

Commodity Futures Trading Commission v Ooki DAO [2022] Northern District of California Case No. 3:22-cv-05416-WHO

Corporation of Dublin v Building and Allied Trade Union (1996) 1 IR 468

D'Aloia v Persons Unknown [2022] EWHC 1723 (Ch)

D'Aloia v Persons Unknown [2025] 1 WLR 821

Daventry District Council v Daventry & District Housing Ltd [2012] 1 WLR 1333

Davis Contractors Ltd v Fareham Urban DC [1956] AC 696

Decro-Wall International v Practitioners in Marketing [1971] 1 WLR 361

Edgington v Fitzmaurice (1885) 29 Ch Div 459

Edwards v Skyways Ltd [1964] 2 WLR 349

Entores v Miles Far East Corporation [1955] 2 QB 327

Esso Petroleum Ltd v Commissioners of Customs and Excise [1975] UKHL 4

Esso Petroleum v Mardon [1976] QB 801

Fibrosa Spolka Akcyjna v Fairbairn Lawson Combe Barbour Ltd [1943] AC 32

Gibson v Manchester City Council [1979] 1 WLR 294

Grainger & Son v Gough (1896) AC 325

Great Peace Shipping Ltd v Tsavliris (International) Ltd [2003] QB 679

Hadley v Kemp [1999] EMLR 589

Hong Kong Fir Shipping Co Ltd v Kawasaki Kisen Kaisha Ltd [1962] 2 QB 26

Irish Life Assurance v Dublin Land Securities Ltd [1989] IR 253

Janesh s/o Rajkumar v Persons Unknown ('CHEFPIERRE') [2022] SGHC 264

Kingstreet Investments v. New Brunswick (Department of Finance) [2007] 1 SCR 3

LAC Minerals v Chevron (6 August 1993, HC)

Lavinia Deborah Osbourne v Persons Unknown [2022] EWHC 1021 (Comm)

Lavinia Deborah Osbourne v Persons Unknown [2023] EWHC 2974 (KB)

Law Society of Ireland v Motor Insurers' Bureau of Ireland [2017] IESC 31

Leaf v International Galleries (1950) 2 KB 86

Lens v Devonshire Club (1914) (The Times)

Lovell & Christmas v Wall (1911) 104 LT 85

Mannai Investment Co Ltd v Eagle Star Life Assurance Ltd [1997] AC 749

Mackin v Deane [2010] IEHC 192

Mersey Steel and Iron Co v Naylor Benzon & Co (1884) 9 App Cas 434

National Provincial Bank v Ainsworth [1965] AC 1175

Newbigging v Adam (1886) 34 Ch D 582

Northern Bank Finance v Charlton [1979] IR 149

Premier Paper Group Ltd v Buchanan McPherson Ltd [2015] EWCA Civ 15

Quoine Pte Ltd v B2C2 Ltd [2020] SGCA (I) 02

R (on the application of Software Solutions Partners Ltd) v Her Majesty's Commissioners for Customs and Excise [2007] EWHC 971

Revenue and Customs v Investment Trust Companies [2017] UKSC 29

Robinson v Harman (1848) 154 ER 363

RTS Flexible Systems Ltd v Molkerei Alois Muller GmbH & Co (UK Production) [2010] 1 WLR 753

Shogun Finance v Hudson [2004] 1 AC 919

Staffordshire AHA v South Staffordshire Waterworks Co [1978] 3 All ER 769

The Sea Angel [2007] 2 Lloyd's Rep 517

The Super Servant Two [1990] 1 Lloyd's Rep 1

Thornton v Shoe Lane Parking [1971] 2 QB 163

Trollope & Colls Ltd v Atomic Power Constructions Ltd [1963] 1 WLR 333

Van Loon v Department of Treasury [2023] Western District of Texas 1:23-CV-312-RP

Vitol SA v Norelf Ltd, The Santa Clara [1996] AC 800

Webster v Cecil (1861) 54 ER 812

Zuphen v Kelly Technical Services [2000] 5 JIC 2401

Books

Adams JN and Brownsword R, *Understanding Contract Law* (5th edn, Sweet & Maxwell)

Amaya A, *The Tapestry of Reason: An Inquiry into the Nature of Coherence and Its Role in Legal Argument* (Bloomsbury Publishing Plc 2015)

Benson P, *Justice in Transactions: A Theory of Contract Law* (Harvard University Press 2019)

Birks P, *Unjust Enrichment* (Oxford University Press 2003)

Brownsword R, *Law, Technology and Society: Re-Imagining the Regulatory Environment* (Routledge 2019)

Chen-Wishart M, *Contract Law* (4th edn, Oxford University Press 2012)

Chen-Wishart M, *Contract Law* (5th edn, Oxford University Press 2015)

Chen-Wishart M, *Contract Law* (7th edn, Oxford University Press 2022)

Clark R, *Contract Law in Ireland* (8th edn, Round Hall Thomson Reuters 2016)

Collins H, *The Law of Contract* (4th edn, Cambridge University Press 2003)

de Filippi P and Wright A, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018)

Fried C, *Contract as Promise: A Theory of Contractual Obligation* (2nd edn, Oxford University Press 2015)

Friel RJ, *The Law of Contract* (Round Hall Press 1995)

McDermott PA, *Contract Law* (2nd edn., Bloomsbury Professional 2017)

McKendrick E, *Contract Law* (9th edn, Palgrave Macmillan 2011)

McKendrick E, *Contract Law* (14th edn, Oxford University Press 2021)

McKendrick E, *Contract Law: Text, Cases, and Materials* (10th edn, Oxford University Press 2022)

Mitchell C, *Interpretation of Contracts* (Routledge-Cavendish 2007)

Morgan J, *Contract Law Minimalism: A Formalist Restatement of Commercial Contract Law* (Cambridge University Press 2013)

Peel E, *Treitel's The Law of Contract* (14th edn, Sweet & Maxwell 2015)

Peel E, *Treitel's The Law of Contract* (15th edn, Sweet & Maxwell 2020)

Ragnedda M and Destefanis G (eds), *Blockchain and Web 3.0: Social, Economic, and Technological Challenges* (Routledge 2019)

Smith SA, *Contract Theory* (Oxford University Press 2004)

Watt G, *Equity and Trusts Law* (Oxford University Press 2021)

Weinrib EJ, *Corrective Justice* (Oxford University Press 2012)

Weinrib EJ, *The Idea of Private Law* (Oxford University Press 2012)

Weinrib EJ, *Reciprocal Freedom: Private Law and Public Right* (Oxford University Press 2022)

Werbach K, *The Blockchain and the New Architecture of Trust* (MIT Press 2018)

Chapters in Books

Allen JG and Hunn P (eds), 'Techno-Legal Supertoys: Smart Contracts and the Fetishization of Legal Certainty', *Smart Legal Contracts: Computable Law in Theory and Practice* (Oxford University Press 2022)

Allen JG, 'Wrapped and Stacked Smart Contracts' in Jason Grant Allen and Peter Hunn (eds), *Smart Legal Contracts: Computable Law in Theory and Practice* (Oxford University Press 2022)

Botterell A, 'Corrective Justice and Contract Law' in Mindy Chen-Wishart and Prince Saprai (eds), *Research Handbook on the Philosophy of Contract Law* (Elgar Publishing 2025)

Brownsword R, 'Smart Contracts: Coding the Transaction, Decoding the Legal Debates' in Philipp Hacker and others (eds), *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019)

Brownsword R, ‘Automated Transactions and the Law of Contract: When Codes Are Not Congruent’ in Michael Furmston (ed), *The Future of the Law of Contract* (Informa Law 2020)

Brownsword R, ‘Smart Contracts: From a Legal Perspective’ in Dário Moura Vicente, Diogo Pereira Duarte and Catarina Granadeiro (eds), *FinTech Regulation and the Licensing Principle* (European Banking Institute 2023)

Brudner A, ‘Hegel and the Crisis of Private Law’ in Drucilla Cornell, Michel Rosenfeld and David Gray Carlson (eds), *Hegel and Legal Theory* (Routledge 1991)

Cannarsa M, ‘Contract Interpretation’ in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019)

Capper D, ‘Remedies for Misrepresentation: An Integrated System’ in Keith Rowley and others (eds), *Commercial Contract Law: Transatlantic Perspectives* (Cambridge University Press 2013)

Carron B and Botteron V, ‘How Smart Can a Contract Be?’ in Daniel Kraus, Thierry Obrist and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Edward Elgar Publishing 2019)

DiMatteo LA, Cannarsa M and Poncibò C, ‘Smart Contracts and Contract Law’ in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019)

Durovic M, ‘What Are Smart Contracts?: An Attempt at Demystification’ in Zvonimir Slakoper and Ivan Tot (eds), *Digital Technologies and the Law of Obligations* (Routledge 2021)

Durovic M and Janssen A, ‘Formation of Smart Contracts under Contract Law’ in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019)

Green S and Sanitt A, ‘The Contents of Commercial Contracts: Smart Contracts’ in Paul S Davies and Magda Raczynka (eds), *Contents of Commercial Contracts: Terms Affecting Freedoms* (Bloomsbury Publishing 2020)

Klimchuk D, ‘Unjust Enrichment and Corrective Justice’ in Neyers JW, McInnes M and Pitel SGA (eds), *Understanding Unjust Enrichment* (Bloomsbury Publishing 2004)

Lee J and Lee J-A, ‘Roadmap to Legal Implications of Web3: An Introduction’ in Lee J and Lee J-A (eds), *Web3 Governance: Law and Policy* (Routledge 2025)

Low KFK, ‘Third Thing or Sixth Sense? I See Ideational Objects?’ in Babie S and Giancaspro M (eds), *Private Law, Digital Assets, and Infrastructure* (Springer 2025)

Marino B and Juels A, ‘Setting Standards for Altering and Undoing Smart Contracts’ in Jose Julio Alferes and others (eds), *Rule Technologies. Research, Tools, and Applications* (Springer International Publishing 2016)

Mik E, ‘The Resilience of Contract Law in Light of Technological Change’ in Michael Furmston (ed), *The Future of the Law of Contract* (Informa Law 2020)

Mik E, ‘The Sense and Nonsense of Smart Contracts’ in Lee J and Lee J-A (eds), *Web3 Governance: Law and Policy* (Routledge 2025)

Murphy L, ‘The Practice of Promise and Contract’ in Gregory Klass, George Letsas and Prince Saprai (eds), *Philosophical Foundations of Contract Law* (OUP Oxford 2014)

Pasa B and DiMatteo LA, ‘Observations on the Impact of Technology on Contract Law’ in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019)

Poncibò C and DiMatteo LA, ‘Smart Contracts: Contractual and Noncontractual Remedies’ in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019)

Sanitt A, ‘Remedies for Smart Legal Contracts: Rectification and Rescission Reconsidered’ in Barış Soyer (ed), *Damages, Recoveries and Remedies in Shipping Law* (Informa Law from Routledge 2023)

Smith SA, ‘Remedies for Breach of Contract: One Principle or Two?’ in Gregory Klass, George Letsas and Prince Saprai (eds), *Philosophical Foundations of Contract Law* (OUP Oxford 2014)

Tjong Tjin Tai E, ‘Smart Contracts as Execution Instead of Expression’ in JG Allen (ed), *Smart Legal Contracts: Computable Law in Theory and Practice* (Oxford University Press 2022)

Weinrib EJ ‘Correctively Unjust Enrichment’ in Chambers R, Mitchell C, and Penner J (eds), *Philosophical Foundations of the Law of Unjust Enrichment* (Oxford University Press 2009)

Weinrib EJ, ‘The Normative Structure of Unjust Enrichment’ in CEF Rickett and Ross Grantham (eds), *Structure and Justification in Private Law: Essays for Peter Birks* (Bloomsbury Publishing Plc 2008)

Weinrib EJ, ‘Legal Formalism’ in Dennis Patterson (ed), *A Companion to Philosophy of Law and Legal Theory* (John Wiley & Sons, Ltd 2010)

Weinrib EJ, ‘The Normative Structuralism of Corrective Justice’ in Hanoch Dagan and Benjamin C Zipursky (eds), *Research Handbook on Private Law Theory* (Edward Elgar Publishing 2020)

Weinrib EJ, ‘The Corrective Justice of Liability for Unjust Enrichment’ in Elise Bant, Kit Barker and Simone Degeling (eds), *Research Handbook on Unjust Enrichment and Restitution* (Edward Elgar Publishing 2020)

Yip M, ‘Mareva Injunction and Crypto Fraud’ in Hans Tijo and Paul S Davies (eds), *Fraud and Risk in Commercial Law* (Bloomsbury Publishing 2024)

Zipursky B, ‘Philosophy of Private Law’ in Jules Coleman and Scott Shapiro (eds), *The Oxford Handbook of Jurisprudence and Philosophy of Law* (Oxford University Press 2002)

Journal Articles

Aldweesh A, ‘BlockTicket: A Framework for Electronic Tickets Based on Smart Contract’ (2023) 18 PLOS ONE e0284166

Allen JG, ‘Wrapped and Stacked: “Smart Contracts” and the Interaction of Natural and Formal Language’ (2018) 14 European Review of Contract Law 307

Barnett RE, ‘Consent Theory of Contract’ (1986) 86 Columbia Law Review 269

Benson P, ‘The Idea of a Public Basis of Justification for Contract’ (1995) 33 Osgoode Hall Law Journal 273

Benson P, ‘The Idea of Consideration’ (2011) 61 University of Toronto Law Journal 241

Biancotti C, ‘What’s Next for Crypto?’ (Social Science Research Network, 21 September 2022) <https://papers.ssrn.com/abstract=4462817> accessed 12 December 2024

Birks P, ‘Unjust Enrichment and Wrongful Enrichment Symposium: Restitution and Unjust Enrichment’ (2000) 79 Texas Law Review 1767

Bonnet S and Teuteberg F, ‘Impact of Blockchain and Distributed Ledger Technology for the Management of the Intellectual Property Life Cycle: A Multiple Case Study Analysis’ (2023) 144 Computers in Industry 103789

Borgogno O and Martino E, ‘Decentralised Autonomous Organisations: Targeting the Potential beyond the Hype’ (2024) 0 Law, Innovation and Technology 1

Botterell A, ‘Property, Corrective Justice, and the Nature of the Cause of Action in Unjust Enrichment’ (2007) 20 Canadian Journal of Law & Jurisprudence 275

Bridgeman C, ‘Corrective Justice in Contract Law: Is There a Case for Punitive Damages Note’ (2003) 56 Vanderbilt Law Review 237

Brownsword R, ‘Regulatory Fitness: Fintech, Funny Money, and Smart Contracts’ (2019) 20 European Business Organization Law Review 5

Bryan M, ‘Justice Callinan’s Judgments in Private Law: Story Telling, Legal Coherence and Corrective Justice’ (2008) 27 University of Queensland Law Journal 29

Cane P, ‘Corrective Justice and Correlativity in Private Law’ (1996) 16 Oxford Journal of Legal Studies 471

Cannarsa M, ‘Interpretation of Contracts and Smart Contracts: Smart Interpretation or Interpretation of Smart Contracts?’ (2018) 26 European Review of Private Law

Cassar DP, ‘The Notion of Mistake in Blockchain-Based Smart Contracts: An Analysis of B2C2 Ltd v Quoine Pte Ltd from a Comparative Perspective’ (2023) 10 European Journal of Comparative Law and Governance 253

Catterwell R, ‘Automation in Contract Interpretation*’ (2020) 12 Law, Innovation and Technology 81

Chan T and Low KFK, ‘DeFi Common Sense: Crypto-Backed Lending in Janesh s/o Rajkumar v Unknown Person (“CHEFPIERRE”)’ (2023) 86 Modern Law Review 1278

Chan T and Low KFK, ‘Post-Scam Crypto Recovery: Final Clarity or Deceptive Simplicity?’ (2023) 139 Law Quarterly Review 379

Chen J and others, ‘Why Do Smart Contracts Self-Destruct? Investigating the Selfdestruct Function on Ethereum’ (2021) 31 ACM Transactions on Software Engineering and Methodology 30:1

Chen-Wishart M, ‘In Defence of Consideration’ (2013) 13 Oxford University Commonwealth Law Journal 209

Cheong MF and Zou M, ‘Resolving Wrongs in Algorithmic Contracting: Applications of the Doctrines of Unconscionability’ (2025) 48(4) University of New South Wales Law Journal (Forthcoming)’ (Social Science Research Network, 1 July 2025) <https://papers.ssrn.com/abstract=5337542> accessed 10 July 2025

Cieplak J and Leefatt S, ‘Smart Contracts: A Smart Way to Automate Performance Technology Explainers’ (2016) 1 Georgetown Law Technology Review 417

Cohney S and Hoffman DA, ‘Transactional Scripts in Contract Stacks’ (2020) 105 Minnesota Law Review 319

Condon RR, ‘After Law Society v MIBI: Contextualism and Contracting in Irish Contract Law’ (2019) 62 Irish Jurist 51

Condon RR, ‘“BIT-PROPERTY”’ (2020) 79 Cambridge Law Journal 224

Cong LW and others, ‘The Dark Side of Crypto and Web3: Crypto-Related Scams’ (14 February 2023) <https://papers.ssrn.com/abstract=4358572> accessed 16 January 2024

Corbin AL, ‘Offer and Acceptance and Some of the Resulting Legal Relations’ (1916) 26 Yale Law Journal 169

Cutts T, ‘Smart Contracts and Consumers’ (2019) 122 West Virginia Law Review 389

Dagan H and Dorfman A, ‘Just Relationships’ (2016) 116 Columbia Law Review 1395

Dagan H and Dorfman A, ‘Justice in Contracts’ (2022) 67 The American Journal of Jurisprudence 1

Dammers W, ‘How to Govern King Code’ in Liisa Albertha Wilhelmina Janssens (ed), *The Art of Ethics in the Information Society: Mind You* (Amsterdam University Press 2016)

Davies PS, ‘Rectifying the Course of Rectification’ (2012) 75 Modern Law Review 412

Davies PS, ‘Rescission for Misrepresentation’ (2016) 75 The Cambridge Law Journal 15

de Graaf TJ, ‘From Old to New: From Internet to Smart Contracts and from People to Smart Contracts’ (2019) 35 Computer Law and Security Review 105322

DiMatteo LA and Poncibó C, ‘Quandary of Smart Contracts and Remedies: The Role of Contract Law and Self-Help Remedies’ (2018) 26 European Review of Private Law

Dowling M, ‘Fertile LAND: Pricing Non-Fungible Tokens’ (2022) 44 Finance Research Letters

Drummer D and Neumann D, ‘Is Code Law? Current Legal and Technical Adoption Issues and Remedies for Blockchain-Enabled Smart Contracts’ (2020) 35 Journal of Information Technology 337

Fairfield JAT and Selvadurai N, ‘Governing the Interface between Natural and Formal Language in Smart Contracts Special Issue: Governing the Digital Space’ (2022) 27 UCLA Journal of Law and Technology 79

Fairfield JAT, ‘Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property’ (2022) 97 Indiana Law Journal 1261

Ferreira A, ‘Regulating Smart Contracts: Legal Revolution or Simply Evolution?’ (2021) 45 Telecommunications Policy 102081

Filatova N, ‘Smart Contracts from the Contract Law Perspective: Outlining New Regulative Strategies’ (2020) 28 International Journal of Law and Information Technology 217

Fuller LL and Perdue WR, ‘The Reliance Interest in Contract Damages: 1’ (1936) 46 Yale Law Journal 52

Gamper F, ‘A Non-Contractual Approach to Smart Contracts’ (2023) 31 International Journal of Law and Information Technology 231

Garon JM, ‘Legal Implications of a Ubiquitous Metaverse and a Web3 Future’ (2022) 106 Marquette Law Review 163

Ghodoosi F, ‘Contracting in the Age of Smart Contracts’ (2021) 96 Washington Law Review 51

Giancaspro M, ‘Is a “Smart Contract” Really a Smart Idea? Insights from a Legal Perspective’ (2017) 33 Computer Law & Security Review 825

Giancaspro M, ‘The Consideration Myth about Smart Contracts’ (2020) 1 ANU Journal of Law and Technology 35

Giancaspro M, ‘“I, Contract”: Evaluating the Mistake Doctrine’s Application Where Autonomous Smart Contracts Make “Bad” Decisions’ (2022) 45 Campbell Law Review 53

Gold AS, ‘A Property Theory of Contract’ (2009) 103 Northwestern University Law Review 1

Gold AS, ‘A Moral Rights Theory of Private Law’ (2010) 52 William and Mary Law Review 1873

Grant DM, Kirby EM and Hawkins SR, ‘Decentralized Autonomous Organizations: To Statutorily Organize or Not?’ (2024) 24 Wyoming Law Review 59

Green L, ‘Law’s Rule’ (1986) 24 Osgoode Hall Law Journal 1023

Green S, ‘Smart Contracts, Interpretation and Rectification’ (2018) Lloyd’s Maritime and Commercial Law Quarterly 234

Green S, ‘The Meaning of Money’ (2020) 44 Brief 12

Guihot M, ‘Coherence in Technology Law’ (2019) 11 Law, Innovation & Technology 311

Hasan HR and others, ‘NFTs for Combating Deepfakes and Fake Metaverse Digital Contents’ (2024) 25 Internet of Things 101133

Herian R, ‘Smart Contracts: A Remedial Analysis’ (2021) 30 Information & Communications Technology Law 17

Hinkes AM, ‘The Limits of Code Deference Symposium: The 20/20 Vision: Blockchain and the Future of Law’ (2020) 46 Journal of Corporation Law 869

Hoffelt C, ‘The Value of Art in the Shape of Nfts: One Step Closer to Perfect Provenance, Market Transparency, and Access to Profit’ (2023) 63 Jurimetrics: The Journal of Law, Science & Technology 355

Horwitz MJ, ‘The Rise of Legal Formalism’ (1975) 19 The American Journal of Legal History 251

Huberman P, ‘Tort Law, Corrective Justice and the Problem of Autonomous-Machine-Caused Harm’ (2021) 34 Canadian Journal of Law & Jurisprudence 105

Hufnagel S and King C, ‘Non-Fungible Tokens: Art and Crime in a Virtual World’ (2023) 5 Criminal Law Review 338

Jiménez F, ‘A Formalist Theory of Contract Law Adjudication’ (2020) 2020 Utah Law Review 1121

Jiménez F, ‘Two Questions for Private Law Theory’ (2021) 12 Jurisprudence 391

Kasatkina M, ‘The Interpretation of Smart Contracts in the EU and the USA Private Law’ (2021) 7 International Comparative Jurisprudence 202

Kelly C, ‘Au Revoir to Merchantable Quality for Consumers—the New Consumer Sales Law in the Consumer Rights Act 2022’ (2023) 30 Commercial Law Practitioner 32

Kilkenny C, ‘Case Note: Osbourne v Persons Unknown and Ozone Network Inc t/a OpenSea Inc [2022] EWHC 1021 (Comm)’ (2023) 30 Commercial Law Practitioner 17

Klass G, ‘How to Interpret a Vending Machine: Smart Contracts and Contract Law’ (2023) 7 Georgetown Law Technology Review 69

Kokorin I, ‘The Decentralisation Defence’ (2025) 57 Computer Law & Security Review 106148

Kolber AJ, ‘Not-So-Smart Blockchain Contracts and Artificial Responsibility’ (2018) 21 Stanford Technology Law Review 198

Lee P-W, ‘Contract Damages, Corrective Justice and Punishment’ (2007) 70 Modern Law Review 887

Leng TK, ‘Who Bears the Risk of Mistake?’ (2004) 20 Computer Law & Security Report 396

Ler PW, 'You've Got Mail: Examining the Postal Rule in the Technological Age' (2019) Singapore Comparative Law Review 35

Loke A, ‘Mistakes in Algorithmic Trading of Cryptocurrencies’ (2020) 83 The Modern Law Review 1343

Low KFK, ‘Bitcoins as Property: Welcome Clarity?’ (2020) 136 Law Quarterly Review 345

Low KFK and Mik E, ‘Lost in Transmission: Unilateral Mistakes in Automated Contracts’ (3 May 2020) <https://papers.ssrn.com/abstract=3591657> accessed 22 March 2024

Luesley A, ‘Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada’ (2019) 19 Asper Review of International Business and Trade Law 155

Ly MK-M, ‘Coining Bitcoin’s “Legal-Bits”: Examining the Regulatory Framework for Bitcoin and Virtual Currencies’ (2014) 27 Harvard Journal of Law & Technology 587

Mayer JI, ‘Unjust Enrichment and the Unwritten Law of Corporate Reorganizations’ (2023) 23 UC Davis Business Law Journal 181

Meyer O, ‘Stopping the Unstoppable: Termination and Unwinding of Smart Contracts’ (2020) 9 Journal of European Consumer and Market Law 17

Mik E, ‘Certainty at Last? A “New” Framework for Electronic Contracting in Singapore’ (2013) 8 Journal of International Commercial Law & Technology 160

Mik E, ‘Smart Contracts: Terminology, Technical Limitations and Real World Complexity’ (2017) 9 Law, Innovation & Technology 269

Mik E, ‘Smart Contracts: A Requiem’ (Social Science Research Network, 7 December 2019) <https://papers.ssrn.com/abstract=3499998> accessed 11 December 2024

Mik E, ‘Contracts in Code?’ (2021) 13 Law, Innovation & Technology 478

Mik E, ‘Smart Contracts: Tales of Trust and Certainty’ (2022) 2022 Technology and Regulation 100

Mik E, ‘Much Ado about Artificial Intelligence or: The Automation of Contract Formation’ (2022) 30 International Journal of Law and Information Technology 484

Moringiello JM and Odinet CK, ‘The Property Law of Tokens’ (2022) 74 Florida Law Review 607

Morrison R, Mazey N CHL, and Wingreen SC, ‘The DAO Controversy: The Case for a New Species of Corporate Governance?’ (2020) 3 Frontiers in Blockchain 1

Nathaniel K and Tey S, ‘Can Smart Contracts Outsmart the Law: The Law of Contract in Light of Smart Contracting’ (2022) 2022 Singapore Comparative Law Review 93

Nicholson A, Udofa K and Collins A, ‘Customer Value Theory and Cryptocurrency Regulation’ (2022) 3 Journal of Law, Technology and Trust

Pacheco M and others, ‘Is My Transaction Done yet? An Empirical Study of Transaction Processing Times in the Ethereum Blockchain Platform’ [2022] ACM Transactions on Software Engineering and Methodology <https://dl.acm.org/doi/10.1145/3549542>

Phang A, ‘Frustration in English Law - A Reappraisal’ (1992) 21 Anglo-American Law Review 278

Priel D, ‘Structure, Function, and Tort Law’ (2020) 13 Journal of Tort Law 31

Reyes CL, ‘If Rockefeller Were a Coder’ (2019) 87 George Washington Law Review 373

Rizos E, ‘A Contract Law Approach for the Treatment of Smart Contracts’ “Bugs”’ (2022) 30 European Review of Private Law 775

Sakharova I, ‘The Power to Contract and the Offer-and-Acceptance Analysis of Contract Formation’ (2024) 37 Canadian Journal of Law & Jurisprudence 261

Savelyev A, ‘Contract Law 2.0: “Smart” Contracts as the Beginning of the End of Classic Contract Law’ (2017) 26 Information & Communications Technology Law 116

Schillig MA, ‘Decentralized Autonomous Organizations (DAOs) under English Law’ (2023) 0 Law and Financial Markets Review 1

Scholz LH, ‘Algorithmic Contracts’ (2017) 20 Stanford Technology Law Review 128

Schuster E, ‘Cloud Crypto Land’ (2021) 84 The Modern Law Review 974

Simpson AWB, ‘Quackery and Contract Law: The Case of the Carbolic Smoke Ball’ (1985) 14 Journal of Legal Studies 345

Sims A, ‘DAOs (Decentralised Autonomous Organisations) v DINOs (DAO in Name Only or Decentralised in Name Only)’ (5 February 2024) <https://papers.ssrn.com/abstract=4716559> accessed 7 May 2024

Sklaroff JM, ‘Smart Contracts And The Cost Of Inflexibility’ (2017) 166 University of Pennsylvania Law Review 263

Stevens R, ‘Crypto Is Not Property’ (2023) 139 Law Quarterly Review

Sumption L, ‘A Question of Taste: The Supreme Court and the Interpretation of Contracts’ (2017) 17 Oxford University Commonwealth Law Journal 301

Tjong Tjin Tai E, ‘Force Majeure and Excuses in Smart Contracts’ (4 May 2018) <https://papers.ssrn.com/abstract=3183637>

Verstappen J, ‘Formation of Contracts’ in Jasper Verstappen (ed), *Legal Agreements on Smart Contract Platforms in European Systems of Private Law* (Springer International Publishing 2023)

Verstappen J, ‘A Smart Contract Taxonomy: An Instrument to Provide Insights in Legal Risks Created by Smart Contract Technology’ (2024) 1 Compact

Verstappen J, ‘Regulating Unfair Commercial Practices in a Smart Contract Context’ (2024) 15 European Journal of Law and Technology

Verstraete M, ‘The Stakes of Smart Contracts’ (2018) 50 Loyola University Chicago Law Journal 743

Webber C, ‘A “Duty to Write” Smart Contracts That Unsophisticated Users Have a “Duty to Read” Note’ (2022) 24 Minnesota Journal of Law, Science and Technology 37

Wei TS, ‘Transnational Transactions on Cryptoasset Exchanges: A Conflict of Laws Perspective’ [2022] Singapore Journal of Legal Studies 384

Weinrib EJ, ‘Legal Formalism: On the Immanent Rationality of Law’ (1987) 97 Yale Law Journal 949

Weinrib EJ, ‘Corrective Justice’ (1991) 77 Iowa Law Review 403

Weinrib EJ, ‘The Gains and Losses of Corrective Justice’ (1994) 44 Duke Law Journal 277

Weinrib EJ, ‘Corrective Justice in a Nutshell’ (2002) 52 The University of Toronto Law Journal 349

Weinrib EJ, ‘Punishment and Disgorgement as Contract Remedies Symposium: Private Law, Punishment, and Disgorgement’ (2003) 78 Chicago-Kent Law Review 55

Weinrib EJ, ‘Civil Recourse and Corrective Justice’ (2011) 39 Florida State University Law Review 273

Werbach K and Cornell N, ‘Contracts Ex Machina’ (2017) 67 Duke Law Journal 313

Wright A, ‘The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges’ (2021) 4 Stanford Journal of Blockchain Law & Policy 152

Yeung K, ‘Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law’ (2019) 82 Modern Law Review 207

Yilmaz T, Sagfossen S and Velasco C, ‘What Makes NFTs Valuable to Consumers? Perceived Value Drivers Associated with NFTs Liking, Purchasing, and Holding’ (2023) 165 Journal of Business Research 114056

Yu G, ‘The Theoretical Foundation of the English Doctrine of Frustration: Efficiency or Justice?’ (2019) 7 City University of Hong Kong Law Review 47

Zhang ZJ, ‘Cryptopricing: Whence Comes the Value for Cryptocurrencies and NFTs?’ (2022) 40 International Journal of Research in Marketing 22

Reports

Cardoso AG, ‘Decentralized Autonomous Organizations - DAOs: The Convergence of Technology, Law, Governance, and Behavioral Economics’ [2023] MIT Computational Law Report <https://law.mit.edu/pub/decentralizedautonomousorganizations/release/1>

Schulp JJ, ‘Crypto Crash: Why the FTX Bubble Burst and the Harm to Consumers’ (*Cato Institute*, 14 December 2022) <https://www.cato.org/testimony/crypto-crash-why-ftx-bubble-burst-harm-consumers> accessed 13 September 2024

UK Law Commission, ‘Decentralised Autonomous Organisations Scoping Paper’ (*Law Commission*) <https://lawcom.gov.uk/document/decentralised-autonomous-organisations-scoping-paper/>

UK Law Commission, ‘Smart Legal Contracts: Advice to Government’ (2021) Law Com No 401

Gleeson S, ‘Legal Considerations Around Smart Contracts: Contracts Between Computer Programs’ (Social Science Research Network, 16 September 2021) <https://papers.ssrn.com/abstract=3925127> accessed 13 May 2025

Media Sources

Chalk A, ‘CS:GO “Dragon Lore” AWP Skin Sells for More than $61,000’ *PC Gamer* (31 January 2018) <https://www.pcgamer.com/csgo-dragon-lore-awp-skin-sells-for-more-than-61000/> accessed 21 March 2024

Katte S, ‘Crypto Rug Pulls Have Slowed, but Are Now More Devastating: DappRadar’ (*Cointelegraph*, 18 April 2025) <https://cointelegraph.com/news/2025-shaping-up-fewer-but-more-impactful-rugpulls-dapp-radar> accessed 16 July 2025

Dale B, ‘MakerDAO Moves to Full Decentralization; Maker Foundation to Close in “Months”’ (*CoinDesk*) <https://www.coindesk.com/tech/2021/07/20/makerdao-moves-to-full-decentralization-maker-foundation-to-close-in-months> accessed 11 December 2024

Irwin K, ‘Rihanna Producer Sells Royalties to “Bitch Better Have My Money” as NFTs’ *Decrypt* (9 February 2023) <https://decrypt.co/120973/rihanna-producer-sells-royalties-to-bitch-better-have-my-money-as-nfts> accessed 13 March 2024

Jafri A, ‘Morgan DF Fintoch Goes Radio Silent after Rugging $31.6M’ (*CryptoSlate*, 25 May 2023) <https://cryptoslate.com/morgan-df-fintoch-goes-radio-silent-after-rugging-31-6m/> accessed 9 June 2023

Kastrenakes J, ‘Nyan Cat Is Being Sold as a One-of-a-Kind Piece of Crypto Art’ *The Verge* (18 February 2021) <https://www.theverge.com/2021/2/18/22287956/nyan-cat-crypto-art-foundation-nft-sale-chris-torres> accessed 14 March 2024

Matthews K, ‘Rare First Printing of US Constitution Sells for Record $43M’ *AP News* (19 November 2021) <https://apnews.com/article/cryptocurrency-technology-lifestyle-business-arts-and-entertainment-b0ab721a52cf20f2dc1a923f2dae3347> accessed 13 December 2024

Packin NG, ‘The CryptoPunk Drama: Is “Code Is Law” Cracking Under Pressure?’ (*Forbes*) <https://www.forbes.com/sites/nizangpackin/2024/09/16/the-cryptopunk-drama-is-code-is-law-cracking-under-pressure/> accessed 17 September 2024

Quarmby B, ‘“Most of Crypto Is Still Junk” and Lacks Use Case — JPMorgan Blockchain Head’ *CoinTelegraph* (30 August 2022) <https://cointelegraph.com/news/most-of-crypto-is-still-junk-and-lacks-use-case-jpmorgan-blockchain-head> accessed 28 July 2023

Websites

‘About’ (*Golem Network*) <https://golem.network/about> accessed 13 December 2024

Afterpattern, ‘Examples of Force Majeure Clauses in Contracts’ (*Afterpattern*) <https://afterpattern.com/clauses/force-majeure> accessed 11 July 2022

Boss Beauties, ‘Boss Beauties Make History At The New York Stock Exchange’ (*Medium*, 27 October 2021) <https://bossbeauties.medium.com/boss-beauties-make-history-at-the-new-york-stock-exchange-715784cbb199> accessed 2 July 2022

Book DAO, ‘Book DAO Co-Author Collective’ <https://www.bookdao.org/> accessed 14 December 2024

Buterin V, ‘DAOs, DACs, DAs and More: An Incomplete Terminology Guide’ (*Ethereum Foundation*, 6 May 2014) <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide> accessed 17 July 2024

CertiK, ‘The Rug Pull Report’ (2023) <https://certik.com/resources/blog/the-rug-pull-report> accessed 28 January 2024

Di Maggio M and Rand B, '"Not a Bunch of Weirdos": Why Mainstream Investors Buy Crypto' (*Harvard Business School*, 17 August 2023) <https://www.library.hbs.edu/working-knowledge/not-a-bunch-of-weirdos-why-mainstream-investors-buy-crypto> accessed 14 September 2023

Everts M and Muller F, 'Will That Smart Contract Really Do What You Expect It To Do?' (TNO) <https://nn8.nl/publications/pdfs/Everts2018WTS.pdf> accessed 5 June 2023

Ghavi A and others, 'A Primer on DAOs' (*The Harvard Law School Forum on Corporate Governance*, 17 September 2022) <https://corpgov.law.harvard.edu/2022/09/17/a-primer-on-daos/> accessed 15 November 2024

'How to Structure DAO Proposals and Build Proposal Processes' (*Aragon*) <https://www.aragon.org/how-to/structure-dao-proposals-and-build-proposal-processes> accessed 2 April 2025

'MakerDAO' <https://makerdao.com/en> accessed 11 December 2024

Morgan Stanley, 'Fintoch Important Notice' <https://www.morganstanley.com/content/dam/msdotcom/global-offices/pdf/Indonesia/Indonesia_Fintoch_Important_Notice.pdf> accessed 1 June 2023

Orenes-Lerma L, 'What Is a Blockchain Validator?' (*Ledger*, 18 April 2023) <https://www.ledger.com/academy/what-is-a-blockchain-validator> accessed 4 April 2024

Prasad E, 'The Brutal Truth about Bitcoin' (*Brookings*, 20 July 2021) <https://www.brookings.edu/articles/the-brutal-truth-about-bitcoin/> accessed 14 May 2023

Saint Olive M and Jagdev S, 'Understanding Slashing in Ethereum Staking: Its Importance & Consequences' (*Consensys*) <https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences> accessed 12 December 2024

'Silk Road: The Dark Side of Cryptocurrency' (21 February 2018) <https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/> accessed 10 December 2024

'Smart Contract Scams | Ethereum Drainers Pose as Trading Bots to Steal Crypto' (*SentinelOne*, 5 August 2025) <https://www.sentinelone.com/labs/smart-contract-scams-ethereum-drainers-pose-as-trading-bots-to-steal-crypto/> accessed 6 August 2025

'Stablecoin Depegging: The What and Why' (*Kraken*, 5 December 2024) <https://www.kraken.com/learn/stablecoin-depegging> accessed 17 December 2024

Szabo N, 'Smart Contracts' (*Universiteit van Amsterdam*, 1994) <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> accessed 3 July 2023

Chainalysis, ‘2024 Crypto Money Laundering Report’ (*Chainalysis*, 15 February 2024) <https://www.chainalysis.com/blog/2024-crypto-money-laundering/> accessed 10 December 2024

Chainalysis, ‘Stablecoins 101: Behind Crypto’s Most Popular Asset’ (*Chainalysis*, 11 December 2024) <https://www.chainalysis.com/blog/stablecoins-most-popular-asset/> accessed 3 June 2025

‘The DAO: What Was the DAO Hack?’ (*Gemini*) <https://www.gemini.com/cryptopedia/the-dao-hack-makerdao, https://www.gemini.com/cryptopedia/the-dao-hack-makerdao> accessed 20 January 2025

‘What Are Gas Fees?’ <https://www.coinbase.com/en-gb/learn/crypto-basics/what-are-gas-fees> accessed 3 March 2025

‘What Can Go Wrong with DAO Investments, and How Should Investigators Respond?’ (*Quantuma*, 15 February 2025) <https://www.quantuma.com/insights/what-can-go-wrong-dao-investments-and-how-should-investigators-respond> accessed 2 April 2025