An assessment of the potential for legal redress for systematic errors in unpermissioned blockchain technology under English Law

By Akrum El Menshawy

A thesis submitted in partial fulfilment of the requirements of Nottingham Trent University for the degree of Doctor of Philosophy

March 2023

Table of Contents

Table of Abbreviations

Bitcoin ATM	Bitcoin Automated Teller Machine
BTO	Bankers Trust Order
CJEU	Court of Justice of the European Union
DAO	Decentralised Autonomous Organisation
DEX	DeFi Exchange
DLT	Distributed Ledger Technology
DOCDEX	Documents-only dispute resolution
EU	European Union
FCA	Financial Conduct Authority
FSA	Financial Services Agency
HKMA	Hong Kong Monetary Authority
ICTs	Information and Communication Technologies
IOSCo	International Organization of Securities Commissions
NFT	Non-Fungible Token
NHS	National Health Service
NPO	Norwich Pharmacal Order
ODR	Online Dispute Resolution
SEC	Securities and Exchange Commission
UDPR policy	Domain names dispute resolution
UK	United Kingdom
VPN	Virtual Private Network
WADA	World Anti-Doping Agency

Abstract

This thesis focuses on the potential for legal redress to be afforded to users who suffer loss resulting from transactions impacted by systematic errors in unpermissioned blockchains. Blockchain technology, which enables a cryptographically secure form of record keeping, is an emerging topic that has the potential to be adopted in many contexts, notably in cryptocurrencies. Unpermissioned blockchain technology provides a unique and decentralised technology in which anyone can participate or alter, and it gives rise to questions as to its compatibility with traditional legal frameworks. The regulatory landscape concerning unpermissioned blockchain technology has hitherto largely focused on the issue of money laundering via cryptocurrencies. However, this has resulted in limited legal protection for users in respect of liability for systematic errors. This thesis will explore the potential for development of the current English legal framework to enable protection to users who suffer loss attributable to systematic errors. Further to this, there shall be the exploration of creative legal solutions for regulating unpermissioned blockchain with the aim of enhanced clarity and legal protection for users in three different contexts: peer to peer, cryptocurrency exchange and DeFi exchange transactions. The public are most likely to encounter unpermissioned blockchain technology in these contexts, through cryptocurrency trading, and therefore risks in each instance may present the most likely case for regulation. Employing a decentred view of regulation, Ostrom's self-management principles are drawn upon as one potential model of self-regulation that might be adapted for unpermissioned blockchain technology.

Acknowledgments

I would like to propose a special thanks to the following people whom if it had not been for them, I would not have been capable of completing this journey. I am eternally indebted to you.

To my supervisory team, without your tireless guidance, support and critique, this project would not be in the same position today.

To both my wife and my mother, you have been there for me at every step of this journey and none of it would have been possible without your unconditional love and support.

Chapter 1: Introduction and Context

1.1: Introduction

The primary focus of this thesis is the potential legal redress that is afforded to the end users of unpermissioned blockchain technology for systematic errors that may occur within the blockchain. In general, blockchain technology is an evolving topic that has vast potential to impact daily life through use, as examples, in the Land Registry,[1] financial transactions[2] and brand loyalty programs.[3] Although subject to contractual underpinnings and restrictions on involvement in the underlying blockchain in those contexts, this thesis concerns unpermissioned blockchain.

Unpermissioned blockchain technology is a decentralised technology that theoretically rests upon shared responsibility for the maintenance of the platform and therefore creates uncertainty in respect of who should bear legal liability in the event of a fault. A cornerstone issue is who could be liable in a decentralised system if systematic errors occur, and a secondary issue is the practicality of legal redress within English law for the end users who may suffer loss resulting from the systematic errors.

This thesis will explore the practicality of current English law in respect of the protection it might provide to users who suffer loss in this context. Further to this, there shall be the exploration of decentred regulation of unpermissioned blockchain with the aim of enhanced clarity and legal protection for users, focusing on circumstances in

[1] HM Land Registry, 'HM Land Registry to explore the benefits of blockchain' (2018) <https://www.gov.uk/government/news/hm-land-registry-to-explore-the-benefits-of-blockchain> Accessed 1st February 2023.

[2] Bank of England Financial Policy Committee, 'Financial Policy Committee Statement from its policy meeting 12 March 2018' (FPC 2018) <https://www.bankofengland.co.uk/-/media/boe/files/statement/fpc/2018/financial-policy-committee-statement-march-2018.pdf?la=en&hash=61059A79F4453B2EFA6BA88A598739DD67FC0CD7> Accessed 1st February 2023, Page 7; Hong Kong Monetary Authority, 'Whitepaper On Distributed Ledger Technology 1.0' (HKMA 2016) <https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf> Accessed 1st February 2023, Page 60.

[3] For more uses of blockchain see Xiwei Xu, Ingo Weber and Mark Staples, *Architecture for Blockchain Applications* (Springer 2019).

which the public is most likely to encounter unpermissioned blockchain technology. The legal solutions discussed in this thesis shall include: the decentred view of regulation and the assessment of Ostrom's self-management principles as an indication of the potential effectiveness of self-regulation within unpermissioned blockchain technology. The discussions will be framed around the different transactional contexts in which users may encounter unpermissioned blockchain technology, namely peer to peer transactions and transactions conducted through exchanges, including decentralised finance exchanges.

This introductory chapter will explore the underlying technology and terminology used in the thesis to provide a basis of knowledge to enable analysis of the unique legal problems that may arise.[4] Following this, will be a literature review and in section 1.5 there will be an explanation of the original contribution to knowledge made by the thesis. Chapter one shall also cover the scope and framing of the research question itself.[5] This section shall combine the contextual elements and identify gaps in the literature to explain how this project will develop. The methodology of the thesis shall then be discussed to highlight the various approaches that shall be employed.[6] Finally, the structure of the entire thesis shall be highlighted.[7]

[4] Alex Hughes and others, 'Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms' (2018) Business Horizons 1551 1, Page 7; Olivier Hari and Ulysse Pasquier, 'Blockchain and distributed ledger technology (DLT): academic overview of the technical and legal framework and challenges for lawyers' (2018) 5 International Business Law Journal 423, Page 423. There is a degree of misunderstanding especially from the public with regards to this topic whereby "a large proportion of society does not yet understand". See, Financial Conduct Authority, 'Cryptoassets: Ownership and attitudes in the UK' (FCA March 2019) <https://www.fca.org.uk/publication/research/cryptoassets-ownership-attitudes-uk-consumer-survey-research-report.pdf> Accessed 1st February 2023, Page 4.
[5] See section 1.7.
[6] See section 1.8.
[7] See section 1.9.

1.2: Key Terminology

1.2.1: What is distributed ledger technology, "DLT"?

A distributed ledger can be defined as "an asset database that can be shared across a network of multiple sites, geographies or institutions."[8] DLT[9] can therefore be defined as the underlying technology that enables…

> *"All participants within a network… (to) have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network."*[10]

[8] Government Office for Science (2015), *Distributed Ledger Technology: beyond block chain*, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 1st February 2023, Page 5.

[9] Blockchain technology is merely a type of Distributed Ledger Technology but there are other forms such as Directed Acyclic Graph (DAG). For more discussion on these different forms of DLT see, Max Thake, 'What's the difference between blockchain and DLT?' (medium.com) <https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd> Accessed 1st February 2023; Demelza Hays, 'Blockchain 3.0 The Future of DLT' (2018) June Crypto Research Report, Accessed 1st February 2023 <https://cryptoresearch.report/crypto-research/blockchain-3-0-future-dlt/>; Volodymyr Babich and Gilles Hilary, 'Blockchain and other Distributed Ledger Technologies in Operations' (2019) 12(2-3) Foundations and Trends in Technology, Information and Operations Management 152; Volodymyr Babich and Gilles Hilary, 'OM Forum – Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology' (2019) 22(2) Manufacturing & Service Operations Management 223.

[10] Government Office for Science (2008). *Distributed Ledger Technology: beyond block chain*, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 1st February 2023, Page 5.

DLT operates via "networks of databases that allow participants to create, disseminate and store information."[11] DLT has the potential to change many industries by enabling transactions to take place peer-to-peer, securely and without the need for a traditional intermediary to authenticate the transaction.[12] The broad spectrum of uses of DLT are not the focus of this thesis, although some uses will be referenced in section 1.6 as a justification for why this topic is of significance, with the main focus being on unpermissioned blockchains in the context of cryptocurrencies.

1.2.2: What is blockchain?

Blockchain technology as mentioned previously is a form of DLT,[13] whereby the information of every transaction is recorded and stored within a "block".[14] The block contains a "hash code" which is a randomly generated numerical series and is

[11] Hong Kong Monetary Authority, 'Whitepaper On Distributed Ledger Technology 1.0' (HKMA 2016) <https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf> Accessed 1st February 2023, Page 10. DLT's potential is not a new concept, however, due to limited usage it remains a novel invention. For further discussion on this see, Alex Hughes and others, 'Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms' (2018) Business Horizons 1551 1, Pages 2 and 7; Olivier Hari and Ulysse Pasquier, 'Blockchain and distributed ledger technology (DLT): academic overview of the technical and legal framework and challenges for lawyers' (2018) 5 International Business Law Journal 423, Pages 423 and 445; Balazs Bodo, Daniel Gervais and Joao Pedro Quintais, 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26 (4) International Journal of Law and Information Technology 311, Page 312; Simply Explained – Savjee, 'How does a blockchain work – Simply Explained' (2017) <https://www.youtube.com/watch?v=SSo_EIwHSd4> Accessed 1st February 2023, Minute 0:18-0:27; For a useful example of how blockchain has wider capabilities than just cryptocurrency, see Chris Baraniuk (BBC), 'Blockchain: The revolution that hasn't quite happened' (2020) <https://www.bbc.co.uk/news/business-51281233> Accessed 1st February 2023.

[12] Hong Kong Monetary Authority, 'Whitepaper On Distributed Ledger Technology 1.0' (HKMA 2016) <https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf> Accessed 1st February 2023, Page 16.

[13] Financial Conduct Authority, 'DP17/3: Discussion Paper on distributed ledger technology' (FCA DP17/3 2017) <https://www.fca.org.uk/publication/discussion/dp17-03.pdf> Accessed 1st February 2023, Page 10; Max Thake, 'What's the difference between blockchain and DLT?' (medium.com) <https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd> Accessed 1st February 2023.

[14] For those in the computer science industry, blockchain was viewed as the long-awaited breakthrough for the technological world. For more information see Don Shin, 'Blockchain: The emerging technology of digital trust' (2019) 45 Telematics and Informatics 101278 <https://www.sciencedirect.com/science/article/pii/S0736585319307701> Accessed 1st February 2023, Page 1; Rishav Chatterjee, 'An Overview of the Emerging Technology: Blockchain' (2017) International Conference on Computational Intelligence and Networks 126 <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8307344> Accessed 1st February 2023, Page 126; Balazs Bodo, Daniel Gervais and Joao Pedro Quintais, 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26 (4) International Journal of Law and Information Technology 311, Page 312.

unique to the transaction and therefore its block. As the crypto asset is transferred from A to B, a block with a unique hash code is created. When B transfers the crypto asset to C a new block with a unique hash code is created and it is bound to the previous block. The hash code present in the latter transaction is bound to the previous hash code in the former transaction. In practice transactions are grouped and then added to the blockchain rather than an update being required after every transaction. This form of coding and the binding of the blocks of transactions provide transparency and validity to each transaction.

There are two forms of blockchain: permissioned and unpermissioned (also referred to as permissionless) blockchain technology.[15] A permissioned blockchain has a central party that is responsible for the maintenance and upkeep of the platform, whereas in an unpermissioned blockchain such responsibility is theoretically shared equally across the network. This fundamental difference in the operation of permissioned and unpermissioned blockchain suggests there may be a need for the legal consequences of fault for systematic errors to differ also.[16] Permissioned blockchain technology is closer to a traditional organisational structure underpinned by extensive contractual arrangements to provide clarity for the issue of liability. Whereas, as will be discussed throughout this thesis, contractual liability is unlikely to be applicable for disputes in unpermissioned blockchain technology.

Permissioned blockchain technology can be used for a variety of reasons. Often it is used as an efficient ledger system for companies that want to retain control over their information. An example of a company that uses permissioned blockchain

[15] Hong Kong Monetary Authority (n 12), Pages 20-21.
[16] Ibid.

technology is Maersk.[17] Their use of the permissioned blockchain technology was to enable "documents for customs clearance (to) flow seamlessly between the involved parties at import and export. They are visible to everyone with guaranteed immutability, privacy and auditability of all the information." It is clear to see why unpermissioned blockchain technology would not have provided a reliable solution for Maersk in this situation due to the lack of control over private information. This is important as some information in a commercial setting may be especially sensitive due to contractual agreements for example.[18] In theory any organisation wanting a uniform ledger could implement permissioned blockchain technology.[19] The potential uses include: land registry,[20] international finance,[21] copyright,[22] data storage,[23] food safety[24] and many more.[25]

[17] Maersk is an International shipping logistics company. Together with IBM they launched a "digital shipping platform" (Jesper Toft Madsen - maersk.com, 'A game changer for Global trade' Sept 2019 <https://www.maersk.com/news/articles/2019/09/20/a-game-changer-for-global-trade> Accessed 1st February 2023) in 2018 that was made possible using Permissioned blockchain technology.

[18] Another example would include Ripple. Ripple contains a cryptocurrency in the form of XRP and provides a platform for global payments. This platform is used by some large organisations as a tool for international payment transfers such as American Express, Santander and MoneyGram. For more information on Ripple, See <https://ripple.com/> Accessed 1st February 2023.

[19] Other examples can include companies, banks or institutions that are willingly operating within the regulatory framework and looking for an efficient system for sharing of information across different locations. For a brief explanation of this see Blockchain Council, 'Permissioned and Permissionless Blockchains: A Comprehensive Guide' <https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/> Accessed 1st February 2023.

[20] HM Land Registry (n 1).

[21] Bank of England Financial Policy Committee, 'Financial Policy Committee Statement from its policy meeting 12 March 2018' (FPC 2018) <https://www.bankofengland.co.uk/-/media/boe/files/statement/fpc/2018/financial-policy-committee-statement-march-2018.pdf?la=en&hash=61059A79F4453B2EFA6BA88A598739DD67FC0CD7> Accessed 1st February 2023, Page 7; Hong Kong Monetary Authority (n 12), Page 60; Xu, Weber and Staples (n 3), Chapter 4.3.

[22] Simon Stokes (Blake Morgan LLP), 'Digital copyright: AI and Blockchain' (2019) <https://www.lexology.com/library/detail.aspx?g=f470dbbf-eb8e-44e5-9d45-1f55bfc25e2a> Accessed 1st February 2023.

[23] Xu, Weber and Staples (n 3), Chapter 4.2.

[24] Ibid, Chapter 4.1; Jennifer McEntire and Andrew Kennedy, *Food Traceability* (Springer 2019), Chapter 10.

[25] For more uses of blockchain see UK Government Chief Scientific Adviser – Mark Walport (Government Office for Science), 'Distributed Ledger Technology: beyond block chain (GS/16/1) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 1st February 2023, Page 4; Xu, Weber and Staples (n 3); Sean Williams (Fool.com), '20 Real-World Uses for Blockchain Technology' (2018) <https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx> Accessed 1st February 2023.

Unpermissioned blockchain technology is extremely novel and untraditional because it does not require a centralised party and is therefore far removed from a permissioned blockchain. In traditional transactions an intermediary such as a bank is required to authenticate transactions and to update and maintain the system. One example is through the use of documentary credits in international trade.[26] The role of the intermediary is vital to offer a degree of protection for the parties involved whereby the payment is only transferred once the bank has the title documents required.[27] Trust is therefore placed in the bank as parties in international trade may not have developed trust in the parties they are dealing with.

Unpermissioned blockchain technology potentially removes the need for this centralised party and instead relies upon cryptographic technology to validate the transactions.[28] As noted, the maintenance and upkeep of the system is distributed equally between the network's users with the responsibility theoretically shared. Trust is placed in the technology rather than the presence of an intermediary.

Permissioned and unpermissioned blockchain technology differ significantly in nature and in legal frameworks.[29] Unpermissioned blockchain technology, which operates in a decentralised manner, presents greater uncertainties as to private liability in the event of a fault in the blockchain, than permissioned blockchain technology and

[26] "A documentary credit is the written promise of a bank, undertaken on behalf of a buyer, to pay a seller the amount specified in the credit provided the seller complies with the terms and conditions set forth in the credit." See Edward Hinkelman, *A short course in International payments: how to use letters of credit, D/P and D/A terms, prepayment, credit, and cyberpayments in international transactions*, (2nd edn, World Trade Press 2009), Chapter 10, Page 50.

[27] Ibid; Uniform Customs and Practice for Documentary Credits (2007 revision, ICC Publication no. 600) (UCP600). For further discussion on documentary letters of credit see, Mohd Hwaidi, 'Letters of credit: model for the illegality exception and for the UCP to address exceptions to the principle of autonomy' (2021) 32(1) Journal of Banking and Finance Law and Practice 26; Mohd Hwaidi and Graham Ferris, 'Switching from paper to electronic bills of lading: Part 2. Fundamental Sociological Structure, Distributed Ledger Technology and Legal Difficulties' (2020) 25(4) Journal of International Maritime Law 297.

[28] Hong Kong Monetary Authority (n 12), Page 20.

[29] Ibid, Page 3; Nathan Dudgeon and Gareth Malna, 'Distributed Ledger Technology: From Blockchain to ICOs' (2018) 37(2) Banking & Financial Services Policy Report 4, Page 4.

will be the main focus of this thesis. The decentralised nature of unpermissioned blockchain technology limits the enforceability of contractual claims as no single entity is necessarily responsible for the platform itself. This combined with the presence of anonymity, a claim enforcement difficultly which will be discussed in the following chapter, present problems in the enforcement of claims based on fault within unpermissioned blockchain technology that may be difficult to resolve using traditional legal dispute resolution mechanisms.

1.2.3: Methods of transaction

The thesis discusses various contexts in which users may encounter crypto transactions involving unpermissioned blockchain technology and uses the term "methods of transaction" for these. The variety of methods of transaction are an essential point of distinction as each method differs from another and thus the landscape of legal liability should differ accordingly.[30] This thesis will primarily focus on 1) peer-to-peer transactions, which involve transacting directly on the blockchain, 2) exchange-based transactions, which involve accessing the platform or crypto assets through a centralised exchange and 3) DeFi Exchange (DEX) transactions, which involve using a platform that can allow peer-to-peer swapping of crypto-assets for other crypto-assets. These three appear to provide the most likely methods of transaction in which a general public user might interacts with a platform utilising unpermissioned blockchain technology.

Although these three methods of transaction will be at the center of focus for this thesis, it is important to note that other methods of transaction exist. For example,

[30] Peder Ostbye, 'Who is Liable if a Cryptocurrency Protocol Fails?' (September 2019) <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3423681> Accessed 1st February 2023, Page 17; Peder Ostbye, 'Who is Liable for an Attack on Cryptocurrency Consensus?' (January 2020) <https://kryptografen.com/opinions/who-is-liable-for-an-attack-on-cryptocurrency-consensus/> Accessed 1st February 2023.

the Bitcoin Automated Teller Machine (Bitcoin ATM) operates in a similar manner to a traditional ATM but enables the buying and selling of Bitcoin[31] and examples can presently be found within commutable distance from every location in the UK.[32]

The distinction between the different methods of transaction will be apparent throughout this thesis. The use of exchanges appears to be one of the more common approaches of transacting with Bitcoin. Although the exchange is not responsible for any faults in the underlying blockchain, they remain a commonly used method of transaction and contain their own faults.[33] According to CoinMarketCap there are over 300 exchanges for cryptocurrency,[34] with other sources referencing in excess of 500.[35] The number of exchanges highlights the likely public demand for purchasing cryptocurrency through an exchange, given the technical complexity of other methods, and it is therefore the most likely source of risk to the public, a point that will be considered in the context of a need for regulation of this sector.

Within the cryptocurrency market, some exchanges themselves have become decentralised and are referred to as DeFi exchanges (also known as DEXs).[36] The DeFi or DEX customers transact on a peer-to-peer basis and are therefore in a different position to general exchange customers discussed above. These DEXs normally operate

[31] bitcoin.org, 'how to buy bitcoin' <https://bitcoin.org/en/buy> Accessed 1st February 2023.
[32] coinatmradar.com, 'Bitcoin ATM Near Me Search' <https://coinatmradar.com/bitcoin-atm-near-me/> Accessed 1st February 2023.
[33] One recent example of how an exchange can be flawed is Sam Bankman-Fried's FTX. For more information on this, see David Yaffe-Ballany (nytimes.com), 'How Sam Bankman-Fried's Crypto Empire Collapsed' (November 2022) <https://www.nytimes.com/2022/11/14/technology/ftx-sam-bankman-fried-crypto-bankruptcy.html> Accessed 1st February 2023.
[34] CoinMarketCap, 'Top Cryptocurrency Exchanges by Trade Volume (Page 4)' <https://coinmarketcap.com/rankings/exchanges/4/> Accessed 1st February 2023.
[35] Cryptimi, 'How many Cryptocurrency Exchanges are there?' <https://www.cryptimi.com/guides/how-many-cryptocurrency-exchanges-are-there> Accessed 1st February 2023; A simple google search of 'bitcoin exchange' will result in 168 million results. On wider scale, googling crypto exchange will provide 465 million results. This highlights not only the volume of results that may be linked to the exchanges but also how much more accessible the exchange route is for general individuals.
[36] Syren Johnstone, *Rethinking the Regulation of Cryptoassets: Cryptographic Consensus Technology and the New Prospect* (Elgar Publishing 2021), Page 169; Vijay Mohan, 'Automated Market Makers and Decentralized Exchanges: A DeFi Primer' (2022) 8 Financial Innovation, Article 20.

on the (unpermissioned) Ethereum blockchain.[37] Some figures suggest that money placed into DeFi platforms including DEXs has increased from twelve billion dollars in 2020,[38] to eight hundred and fifty four billion dollars in 2022.[39] The incentive to invest in these DeFi platforms is only exacerbated by the "historically low or sub-zero interest rates",[40] and the wider sector of traditional exchanges experiencing numerous hacks.[41] Again, the position in respect of DEXs will be analysed separately in this thesis.

In this thesis, the end users in the peer-to-peer method of transaction will be referred to as "peer-to-peer users". The end users in exchange-based transactions will be referred to as "exchange customers" and the users of the DEX will be referred to as "DEX customers". Further key roles will be explored in section 1.3. Peer-to-peer users interact directly with the platform using unpermissioned blockchain technology. They can also be involved in the maintenance and up-keep of the platform and may even validate transactions. The maintenance of the platform is theoretically shared amongst all peer-to-peer users. This is the case in the traditional setting where peer-to-peer users interact with the technology to access the network. This thesis makes the distinction between a peer-to-peer user and a miner or coder, although there may be overlaps in these roles. In exchange-based transactions, users would be regarded as exchange customers as their interaction with the platform is through the exchange. The exchange

[37] Vijay Mohan, 'Automated Market Makers and Decentralized Exchanges: A DeFi Primer' (2022) 8 Financial Innovation, Article 20, Page 4. For further potential uses of the Ethereum blockchain see, Emre Yavuz and others, 'Towards secure e-voting using ethereum blockchain' (2018) 6th International Symposium on Digital Forensic and Security (ISDFS) <https://ieeexplore.ieee.org/abstract/document/8355340> Accessed 1st February 2023.
[38] Tom Wilson (reuters.com), 'Crime at crypto *DeFi* sites hits $10.5bln in 2021, research shows' (November 2021) <https://www.reuters.com/technology/crime-crypto-defi-sites-hits-105-bln-2021-research-shows-2021-11-18/> Accessed 1st February 2023.
[39] Nansen.ai, 'DeFi Statistics [updated in 2023]' (December 2022) <https://www.nansen.ai/guides/defi-statistics-in-2022> Accessed 1st February 2023.
[40] Wilson (n 38).
[41] Although it is worth noting that DeFi has been notorious for hacks in recent years also. See, (defillama.com), 'Hacks' (January 2023) <https://defillama.com/hacks> Accessed 1st February 2023; (Protos.com), 'Top DeFi hacks and exploits of 2022' (December 2022) <https://protos.com/top-defi-hacks-and-exploits-of-2022/> Accessed 1st February 2023; Jeffrey Gogo (beincrypto.com), 'Top Ten DeFi Hacks of 2022: Hackers Get More Daring' (September 2022) <https://beincrypto.com/top-ten-defi-hacks-2022-hackers-daring/> Accessed 1st February 2023.

could potentially operate via the peer-to-peer network and so may also be classed as a peer-to-peer user. This distinction is important as some aspects discussed throughout this thesis will relate to one specific group or may relate equally to peer-to-peer users, exchange customers and DEX customers. To develop on from this, further terminology will be explored.

1.2.4: What is consensus?

Similar to a traditional ledger,[42] a distributed ledger needs amending to provide an accurate and up-to-date record. Within a distributed ledger, transactions are pooled and when the ledger is updated a block will be added.[43] To validate each block on the Bitcoin blockchain a proof-of-work validation method, based on consensus, is normally used. "Consensus" requires the whole network to accept the updated transaction, unlike in a traditional ledger whereby an authorized individual could update the ledger without consensus.[44]

Validated blocks record whether the property transferred belongs to the seller and whether the property exists. A vital aspect of the validation process is mining. Mining is the completion of complex cryptographic algorithms for the purpose of validation of each block. Theoretically, any user with the necessary computational power can act as a miner for the purpose of an unpermissioned blockchain. Often this costly task is compensated with virtual tokens in the process of mining. In Bitcoin, the

[42] According to the Cambridge Dictionary, 'Ledger' (2020) <https://dictionary.cambridge.org/dictionary/english/ledger> Accessed 1st February 2023, a ledger is defined as "a book in which things are regularly recorded, especially business activities and money received or paid". The traditional ledger is simply a record of activities, often financial. This record is usually an individual copy.

[43] (gemini.com), 'How a Block in the Bitcoin Blockchain Works' (March 2022) <https://www.gemini.com/cryptopedia/what-is-block-in-blockchain-bitcoin-block-size> Accessed 1st February 2023.

[44] Christina Majaski (Investopedia), 'Distributed Ledgers' (2019) <https://www.investopedia.com/terms/d/distributed-ledgers.asp> Accessed 1st February 2023. For a further discussion of recent developments in consensus algorithms see, Huanliang Xiong and others, 'Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms' (2022) 14 Future Internet 47 <http://dx.doi.org/10.3390/fi14020047> Accessed 1st February 2023.

miners/validation nodes currently receive 6.5 Bitcoins for the completion process of mining each new block.[45] This computational process is time and energy resource-intensive but is a common component of the operation of the technology, primarily when proof-of-work is the validation method.[46]

Within permissioned blockchain technology, in contrast, the centralised party is responsible for the validation process. The validation nodes will be trusted parties, often employed by the controlling party to complete the validation process and upload an updated form of the ledger for the peer-to-peer users to access. Access to a permissioned blockchain is restricted to only the trusted parties. Commonly permissioned blockchain technology is referred to as private because of the restricted access.[47] In the validation process for example, a permissioned blockchain does not require the complex cryptographic algorithms to be completed prior to validation. Instead, trusted validating nodes complete the transaction and send this updated version to all the other nodes, to ensure uniformity. The system's operations can remain private and, given their greater formality, liability for faults may be addressed in contract.

[45] Hossein Jahanshahloo, Felix Irresberger and Andrew Urquhart, 'Bitcoin Under the Microscope' (November 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4273839> Accessed 1st February 2023, Page 6. It is worth noting that in 2016 the sum awarded was twenty-five Bitcoins. The original sum was fifty Bitcoins but the value of the reward halves every four years or every 210,000 blocks mined and so will reduce over time. For more discussion see, UK Government Chief Scientific Adviser – Mark Walport (Government Office for Science), 'Distributed Ledger Technology: beyond block chain (GS/16/1) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 1st February 2023, Page 5.

[46] For further discussion of the environmental impact of mining within Bitcoin see, Liana Badea and Mariana Claudia Mungiu-Pupazan, 'The Economic and Environmental Impact of Bitcoin' (2021) 9 IEEE 48091; Alex de Vries, 'Bitcoin boom: What rising prices mean for the network's energy consumption' (2021) 5(3) Joule 509; Anh Ngoc Quang Huynh and others, 'Energy Consumption and Bitcoin Market' (2022) 29 Asia Pacific Financial Markets 79.

[47] Where-as unpermissioned blockchain technology is regarded as public. Although this does not always have to be the case.

1.2.5: What is Bitcoin?

Bitcoin is at the time of writing this thesis, the most well-known platform utilising unpermissioned blockchain technology.[48] Although originally perceived as an overtly anti-establishment approach to finance,[49] Bitcoin has experienced popularity and has been authorized as legal tender in El Salvador and Central African Republic.[50] Currently, cryptocurrencies such as Bitcoin are not recognised as a legal currency within England, although popular as investments.

From the outset of Bitcoin, the lack of a centralised trusted party, for example a bank, is recognised as a core distinctive component.[51] Developing as a response to the 2007-8 financial crash, Bitcoin seeks to place the trust in the technology rather than a corporation, industry or individual.[52] The lack of trust towards traditional intermediaries plays a heavy role in the operational elements of Bitcoin, such as the potential to be anonymous,[53] the trust in the technology and the cross-border nature of this unpermissioned blockchain.[54] Bitcoin, a "new form of money",[55] operates as a

[48] Hong Kong Monetary Authority (n 12), Page 6; Balazs Bodo, Daniel Gervais and Joao Pedro Quintais, 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26 (4) International Journal of Law and Information Technology 311, Page 312; Alex Hughes and others, 'Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms' (2018) Business Horizons 1551 1, Page 2.
[49] Hong Kong Monetary Authority (n 12), Page 34.
[50] Global Legal Research Directorate, 'Regulation of Cryptocurrency Around the World' (2018) The Law Library of Congress, Global Research Centre <https://tile.loc.gov/storage-services/service/ll/llglrd/2018298387/2018298387.pdf > Accessed 1st February 2023; BBC, 'Bitcoin becomes official currency in Central African Republic' (27th April 2022) <https://www.bbc.co.uk/news/world-africa-61248809> Accessed 1st February 2023.
[51] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (bitcoin.org) <https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf> Accessed 1st February 2023.
[52] Ibid. It is relevant to also distinguish Bitcoin and other cryptocurrencies of a similar model from that of a 'stablecoin' which would be cryptocurrencies that are tied to the value of a commodity to reduce the volatility of value. For further information see, (coinbase.com), 'What is a stablecoin?' (2022) <https://www.coinbase.com/learn/crypto-basics/what-is-a-stablecoin> Accessed 1st February 2023.
[53] Gemma Variale, 'Market poll: the best way to regulate' (2013) Oct International Financial Law Review 1, Paragraph 4.
[54] Zeljko Bjelajac and Momcilo Bajac, 'Blockchain Technology and Money Laundering' (2022) 39(2) Pravo-Teorija I Praska 21, Pages 22-25.
[55] Dominic Frisby, *Bitcoin: The Future of Money?* (Unbound 2014), Page XXV.

cryptocurrency[56] although such a categorisation may not be so definitive.[57] It was intended as a payment system,[58] used as both an investment asset[59] and virtual currency[60] and therefore perceived as both. The capability of Bitcoin and other cryptocurrencies to be categorised in numerous opposing manners inhibits the potential for legal clarity, wider applicability, [61] and legal flexibility[62] across jurisdictions.[63] The next section will explore the key roles within unpermissioned blockchain technology to determine whether any potential hierarchy of liability might arise in cases of fault.

1.3: Key roles

Allocation of responsibility is important for the purposes of liability. To be able to determine a party's responsibility, one may assess the role that they had in the action.

---

[56] Cambridge Dictionary, 'Cryptocurrency' (2023) <https://dictionary.cambridge.org/dictionary/english/cryptocurrency>Accessed 1st February 2023 defines cryptocurrency as "a digital currency produced by a public network, rather than any government, that uses cryptography to make sure payments are sent and received safely."

[57] Bank of England Financial Policy Committee, 'Financial Policy Committee Statement from its policy meeting 12 March 2018' (FPC 2018) <https://www.bankofengland.co.uk/-/media/boe/files/statement/fpc/2018/financial-policy-committee-statement-march-2018.pdf?la=en&hash=61059A79F4453B2EFA6BA88A598739DD67FC0CD7> Accessed 1st February 2023, Page 7; Jeffrey Dorfman (Forbes.com), 'Bitcoin is an Asset, not a Currency' (2017) <https://www.forbes.com/sites/jeffreydorfman/2017/05/17/bitcoin-is-an-asset-not-a-currency/#6f4277d62e5b> Accessed 1st February 2023.

[58] Nakamoto (n 51).

[59] An investment asset can be defined as "homogenous commodities… (that) cannot be differentiated". See, Raya Mamarbachi, Marc Day and Giampiero Favato, 'Art as an alternative investment asset' 2008 Accessed 1st February 2023 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1112630> Page 5. It can include a "variety of assets", and so may include cryptocurrency. See, Financial Conduct Authority, 'PS19/4: Asset Management Market Study - further remedies'' (FCA PS19/4 2019) <https://www.fca.org.uk/publication/policy/ps19-04.pdf> Accessed 1st February 2023, Page 4.

[60] A virtual currency can be defined as "a digital representation of value… not issued or guaranteed by a central bank… but is accepted… as a means of exchange and which can be transferred, stored and traded electronically." See, Dr Robby Houben, 'Cryptocurrencies from a money laundering and tax evasion perspective' (2019) 30(5) International Company and Commercial Law Review 261, Page 265.

[61] It is acknowledged that different methods of enforcement of the law will require different levels of specificity of the law. In theory if prosecution is the key form of enforcement, then the law should be clearly defined to provide legal clarity. If prosecution is not the outcome for the law, then the law may be vaguer and categorise more generally. For more information see Robert Baldwin, Martin Cave and Martin Lodge, *Understanding regulation: theory, strategy, and practice* (2nd edn, Oxford University Press 2012), Pages 230-231.

[62] Common examples can be seen with international regulation that is then transposed into domestic law to differing extents depending on the jurisdiction. The underlying legal principles may be uniform but the practical implementation of them is up to the discretion of the differing jurisdictions. For more information see Robert Baldwin, Martin Cave and Martin Lodge, *Understanding regulation: theory, strategy, and practice* (2nd edn, Oxford University Press 2012), Pages 373-387.

[63] For an example where legal efficiency can be enhanced through regulatory categorisation see the discussion of online content and the separation of categories, House of Lords Paper (Select Committee on Communications), Regulating in a digital world, 2nd report of Session 2017-2019 (March 2019), HL Paper 229, Page 48.

In traditional systems different roles carry different responsibilities. Failure to adhere to such responsibilities could result in termination of the contract and potentially liability in damages for those at fault [64] For example, company directors are responsible for the management of an organisation and are subject to fiduciary duties, which can result in liability.[65] However, as discussed below, no such hierarchy theoretically exists within unpermissioned blockchain technology.[66]

For the unpermissioned blockchain technology to run effectively, various roles must be filled which include: Creators, Coders and Miners. Whilst this is not an exhaustive list, these roles are the only groups that could likely be susceptible to liability as they are involved in the formation of the platform (creators), the coding (coders) and the validation of the transactions (miners). Other roles in an unpermissioned blockchain technology platform are not likely to be as significant for the purpose of liability. For example, the exchanges will not be liable for coding errors on the peer-to-peer method of transaction unless they operate in one of these key peer-to-peer roles and so will not be discussed for the purpose of this section.

Whilst one of the underlying principles of unpermissioned blockchain technology is the decentralised, distributed and equal control across the whole network, in reality different roles have differing levels of control. However, because all of them need to operate together by consensus, theoretically the control is still insufficient for any one party to manipulate or damage the platform.[67]

The potential responsibility of the various roles can subsequently be applied to the theories of liability to suggest who theoretically could be liable for systematic errors

[64] This may be dependent on the terms of the contract, the general principles of law and issues such as vicarious liability, to name a few.
[65] S171-177 Companies Act 2006.
[66] Hong Kong Monetary Authority, 'Whitepaper On Distributed Ledger Technology 2.0' (HKMA 2017) <https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20171025e1a1.pdf> Accessed 1st February 2023, Page 104.
[67] bitcoin.org, 'What are the advantages of Bitcoin?' <https://bitcoin.org/en/faq#what-are-the-advantages-of-bitcoin> Accessed 1st February 2023.

within unpermissioned blockchain technology.[68] It is important from a legal perspective to determine whether a potential hierarchy exists. If some form of responsibility can be attributed to the roles within unpermissioned blockchain technology, then it would increase its compatibility with a traditional legal framework.[69]

It appears logical to explain the various roles in chronological order of operation. Therefore, the first role that will be discussed is that of a creator.[70] It is important at the outset of these discussions to note that a legal entity (be that an individual or other legal person such as a company) may fill multiple roles simultaneously and may operate within different roles over time.

One prime example of a creator within unpermissioned blockchain technology would be the creator of Bitcoin, Satoshi Nakamoto.[71] As suggested above, creators and coders can overlap, and Satoshi would be an example of this. Creators are present at the formation of the blockchain and may take certain decisions in relation to the early coding, internal rules of the system and potentially impact the value of the cryptocurrency due to the novelty and structure of the formation of the platform itself.[72] For example the novelty of Bitcoin's structure has resulted in increased notoriety and arguably has created a large part of its value. Due to the decentralised nature of unpermissioned blockchain technology a creator may step away from any association with the platform almost immediately after its formation. This creator would then be reliant on other parties seeing value in the platform and acting as coders and nodes

[68] See Chapter 3.
[69] Hong Kong Monetary Authority (n 66), Pages 103-104. Additionally, societal usage may increase where there is a greater understanding of the structural operation of the platform using the technology, societal usage may increase.
[70] It could be suggested that the creator and coder would work simultaneously at the formation of the platform or may be the same person. However, for the purposes of this chapter the creator shall be discussed first.
[71] For an interesting discussion of who Satoshi Nakamoto is see, bitcoin.com (Avi), 'Who is Satoshi Nakamoto? An Introduction to Bitcoin's Mysterious Founder' (March 2020) <https://news.bitcoin.com/satoshi-nakamoto-founder-of-bitcoin/> Accessed 1st February 2023.
[72] Malcolm Campbell-Verduyn, *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018), Page 49.

(discussed below) within the system to keep it running. This is what many believe happened with Bitcoin and Satoshi Nakamoto.[73] In contrast, the co-founder of Ethereum, Vitalik Buterin is well-known as remaining active in the cryptocurrency community and remains a key figure in the development of the Ethereum platform.[74]

This untraditional system does not give value to the creator of the platform as traditionally an individual entity will not assert any sense of ownership or control.[75] Whilst ownership is possible for the individual coins within cryptocurrency for example, ownership over unpermissioned platforms appears uncommon. This can explain why many potential uses of blockchain technology often refer exclusively to the *permissioned* blockchain due to the centralised component.[76] In contrast, the shared responsibility and control in unpermissioned blockchain technology goes against the concept of a centralised platform. Consequently, the original creators of the platform may be removed from liability early on as the platform develops.

As shown above, the original creator of Bitcoin can also be regarded as a coder of Bitcoin and subsequently a developer as they are developing the platform through updating code and fixing issues.[77] For the purpose of this chapter, that is why the term "creator" is the creator or original creators, whereas a "coder" is anyone since who has coded for the platform.[78] The original coding may have been altered over time by many individuals and so this is why the creator and the coder should be distinguished.[79]

---

[73] bitcoin.com (Avi) (n 71).
[74] Brayden Lindrea, 'Vitalik reveals a new phase in the Ethereum roadmap: The Scourge' (2022) <https://cointelegraph.com/news/vitalik-reveals-a-new-phase-in-the-ethereum-roadmap-the-scourge> Accessed 1st February 2023.
[75] bitcoin.org, 'Who created Bitcoin?' <https://bitcoin.org/en/faq#who-created-bitcoin> Accessed 1st February 2023.
[76] For example, the previously mentioned potential of adopting permissioned blockchain technology for use in the land registry would likely be impractical if unpermissioned blockchain technology was instead relied upon as the government would not retain control and oversight. For further information see, HM Land Registry (n 1).
[77] bitcoin.org, 'Who controls the Bitcoin network?' <https://bitcoin.org/en/faq#who-controls-the-bitcoin-network> Accessed 1st February 2023.
[78] In theory they could both be accurately described as 'developers' of the platform.
[79] For more discussion on how code can be updated and the process of such updates see, bitcoin.org, 'Code Review' <https://bitcoin.org/en/development> Accessed 1st February 2023.

Therefore, potentially it becomes a difficult question of who creates a flawed piece of coding. If it can be traced back to the original coding of Satoshi that renders a platform susceptible to a hack or malfunction,[80] would it be fair to regard Satoshi as liable? Or would the responsibility fall on recent coders for failing to change it? This is a difficult aspect of liability within unpermissioned blockchain technology and any proposed form of legal redress in Chapter 4 will have to address unique issues such as this.

If a fault exists within a particular set of code, then said coder might reasonably be considered liable for the fault, although there would be some difficulties.[81] Much like the anonymity that is prevalent within unpermissioned blockchain technology,[82] coders are not always easily identifiable.[83] Whilst some coders incorporate signatures within code that they incorporate or develop, this is not always the case. It has even been suggested that the anonymity of coders may be an important right of privacy for some coders.[84] Furthermore, it could overburden coders within the system. For example, if coders are following a generally accepted form of code, or industry practice it could be unfair to regard them as liable should there be a fault later. After what period would the original coder be removed from liability and at what stage would the new coders bear

[80] For examples of some coding errors on blockchains see, David Hamilton (coincentral.com), 'The Biggest Crypto Programming Errors of All Time' (2018) <https://coincentral.com/biggest-crypto-programming-errors/> Accessed 1st February 2023; Shabna Madathil and Sai Kanduri, 'Learn best practices for debugging and error handling in an enterprise-grade blockchain application' (2022) <https://developer.ibm.com/blogs/debugging-and-error-handling-best-practices-in-a-blockchain-application/> Accessed 1st February 2023; Anca F (coindoo.com), 'The Biggest Crypto Programming Errors in History' (2019) <https://coindoo.com/the-biggest-crypto-programming-errors-in-history/> Accessed 1st February 2023.

[81] For a discussion of this in the context of whether coders could be subject to a fiduciary duty see, Angela Walch, 'In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains' in Ioannis Lianos, Phillipp Hacker, Stefan Eich and Georgios Dimitropoulos (ed) *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019).

[82] Bjelajac and Bajac (n 54), Page 27. The issue of anonymity will be discussed in the following chapter in section 2.3.

[83] For a discussion on what can be done to limit the anonymity of coders see, Aylin Caliskan-Islam and others, 'De-anonymizing Programmers via Code Stylometry' (2015) Proceedings of the 24th Security Symposium <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-caliskan-islam.pdf> Accessed 1st February 2023.

[84] Ibid, Page 255.

the responsibility to change the code should it become outdated? As discussed in Chapter 4 these issues are only recently starting to be considered by the courts.

Miners fulfil another key role within unpermissioned blockchain technology in validating transactions and updating the ledger.[85] There has already been the discussion of how a miner tends to operate, where they are essentially using their computer to run coding with the hash code and validation process being automated software. For miners, the key issue would be what transactions they could be held accountable for regarding the automated nature of mining and whether responsibility would be viewed individually or collectively.[86]

Theoretically, a group of dishonest miners could authorise incorrect transactions for their own benefit and this problem will be covered in Chapter 4 from a liability perspective.[87] However, without the intention and control to manipulate transactions, can miners be held accountable? If the program is just running in the background and an error happens, it may not be fair to hold the miner liable unless they are negligent. Alternatively, the miner's computer could be regarded as acting as a vessel for the execution of the code, then potentially the coder could be more blameworthy than the miner. This would then raise the issues discussed in the context of the liability of coders above, thus meaning that each case may turn on its own facts.[88]

In more traditional organisational structures, for example if goods are not of satisfactory quality,[89] or if a product is defective[90] the purchaser will have a variety of

[85] Aron Laszka, Benjamin Johnson and Jens Grossklags, 'When Bitcoin Mining Pools Run Dry: A Game-Theoretic Analysis of the Long-Term Impact of Attacks Between Mining Pools' (2015) <http://fc15.ifca.ai/preproceedings/bitcoin/paper_13.pdf> Accessed 1st February 2023, 3.4.
[86] For a similar example see the discussion of liability for self-driving vehicles, Chris Reed, Elizabeth Kennedy and Sara Nogueira Silva, 'Responsibility, Autonomy and Accountability: legal liability for machine learning' (2016) Microsoft Cloud Computing Research Centre Paper presented at the 3rd Annual Symposium <https://cebcla.smu.edu.sg/sites/cebcla.smu.edu.sg/files/Reed%20Machine%20learning%20liability%20SSRN-id2853462.pdf> Accessed 1st February 2023.
[87] See section 4.2.1.
[88] Hong Kong Monetary Authority (n 66), Page 86.
[89] Section 9 Consumer Rights Act 2015 c15.
[90] Section 2 Consumer Protection Act 1987.

rights.[91] If the purchaser chooses to sue, they will often pursue the party with the deepest pockets out of the seller or manufacturer for example, as not only will these companies be in a better position to pay damages, but also they would be more accessible than suing the individual that may have caused the fault. Due to vicarious liability, where an employee is negligent the company will be liable for the loss caused.[92] The difficulty in unpermissioned blockchain technology within the peer-to-peer method specifically is that there is no centralised party. Therefore, should a fault arise that may attract liability, the potential claimant may have difficulty in establishing who is liable. They are most likely to have to sue on a noncontractual basis and it might be difficult to prove, for example determining the responsible role within the system and who fulfilled it.

Regarding the DEX method of transaction, there is some debate as to the extent of decentralisation that is present.[93] This will be discussed throughout the thesis and will essentially depend on the true operation of the DEX and whether they are closer to an exchange or closer to a party within the peer-to-peer method in respect of control and liability. For the purpose of this chapter, they will be viewed as more akin to an exchange, but further discussion of the DEX in respect of the hierarchy is not required at this stage.

[91] Sections 19-24 Consumer Rights Act 2015 c15.
[92] *Dubai Aluminium Co Ltd* v *Salaam* [2002] UKHL 48, [2003] 2 AC 366, Para [21].
[93] Miles Kruppa, 'DeFi projects rife with hidden risks, global regulatory body warns' (March 2022) <https://www.ft.com/content/b0c581c8-96b2-4c34-abcc-5189d7283891> Accessed 1st February 2023.

1.3.1: Hierarchy

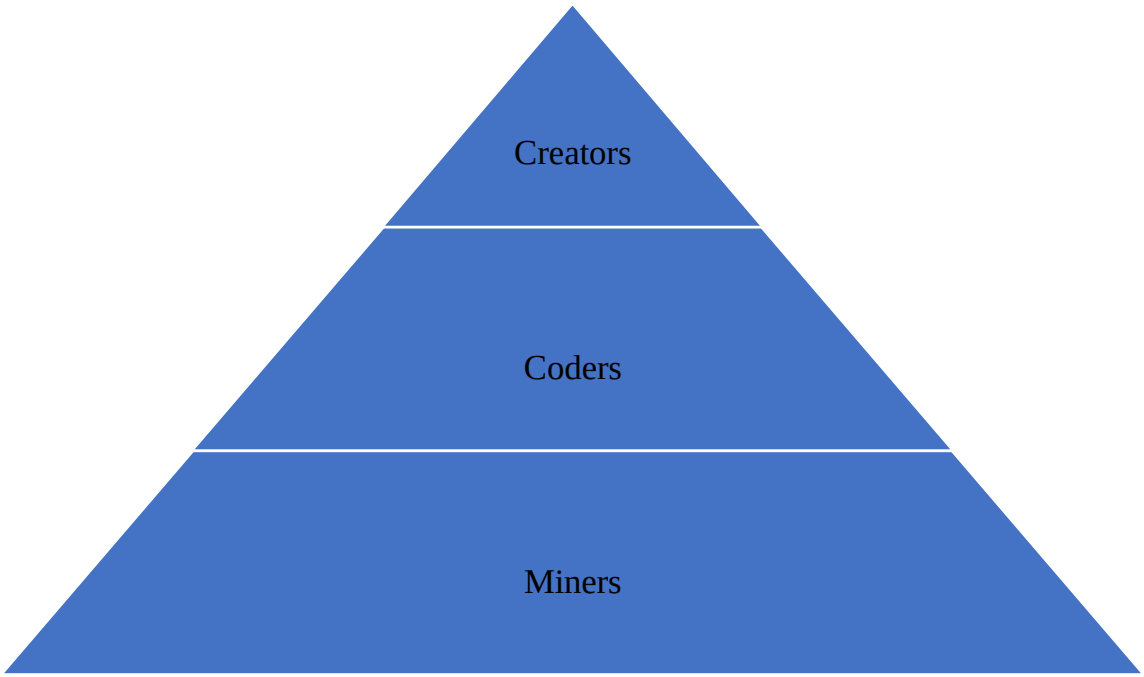

Figure 1: Hierarchy of unpermissioned Blockchain technology[94]

The ordering in Figure 1 is based on a timeline of involvement perspective. The Creators are the original party that forms the platform and so are located at the top. The Coders may help to build the platform and develop it to a point of prominence but there may be some overlap with Creators at this stage. The Miners are a key part of the current operation of the platform and so follow the Creators and Coders. By contrast, in a more traditional structure, the owners of a company would sit at the top of the liability pyramid and there would be a structured hierarchy of directors, managers and other employees. As there is no party that owns unpermissioned blockchain technology or any platforms using the technology, the closest party to an owner could be a creator. As mentioned previously, creators may have very little to do with the platform post creation and so that can be an issue.

By contrast, the directors of a company would have a significant degree of control, followed by some other senior staff and then the rest of the general staff of the

[94] Based on an adaptation of a hierarchy proposed in Hong Kong Monetary Authority (n 66), Page 104.

company and all would be protected by the corporate veil.[95] This is a key distinction between the organisational structure of a company and that of a platform utilising unpermissioned blockchain technology. Whilst unpermissioned blockchain technology does not provide a replicated organisational structure, the closest proposed hierarchy to that structure would be where the coders sit above the miners who in turn have more control than the peer-to-peer users that do not fulfil roles of coding or mining. Some issues with liability and these roles were discussed in the previous section and will be returned to in Chapters 3 and 4 so do not need to be a focus here. In respect of DEXs, much could depend on the nature of how they operate as DEXs have been shown to be a prevalent source of coding errors,[96] although predominantly the errors are in the exchanging bridge rather than the blockchain code.[97]

Two main issues arise from the hierarchy in Figure 1. The first issue is predicated on the concept that responsibility of maintenance is equally shared amongst peer-to-peer users despite differing roles having different levels of importance, as suggested previously. Measures such as cryptography and the permanence of the ledger may prevent an abuse of power within the platform and thus limit the applicability of a hierarchy.[98] The second key issue for any proposed hierarchy is that errors within unpermissioned blockchain technology would be highly fact and case sensitive and so a uniform hierarchy is highly impractical.[99] Consequently, this thesis makes no assertion

[95] *Salomon* v *A Salomon & Co Ltd* [1896] UKHL 1; *Prest* v *Petrodel Resources Limited and others* [2013] UKSC 34.
[96] For an example see, Haseeb Shaheen (cryptopolitan.com), 'OptiFi: Solana-based DEX loses $661,000 due to programming error' (September 2022) <https://www.cryptopolitan.com/optifi-loses-66100-due-to-coding-error/> Accessed 1st February 2023.
[97] For some discussion on this see, Decrypt.com, 'The Problem with Decentralized Exchanges – and How to solve it' (November 2021) <https://decrypt.co/84575/the-problem-with-decentralized-exchanges-and-how-to-solve-it> Accessed 1st February 2023.
[98] For a discussion on some of the security aspects of blockchain see, Xiaoqi Li and others, 'A survey on the security of blockchain systems' (2020) 107 Future Generation Computer Systems 841. For the discussion on the security aspects that protect a platform using unpermissioned blockchain technology see sections 2.1 and 2.2.
[99] For a brief discussion of how unpermissioned blockchain technology makes no reference to any hierarchy see, Hong Kong Monetary Authority (n 66), Page 104.

that such a hierarchy should be sought after for making decisions regarding liability. The following section will explore the most relevant sources of note relating to this thesis.

1.4: Literature Review

The developing area of blockchain as a topic is gaining more focus from academics. Although there are numerous sources that broadly relate to this area of blockchain, this section will focus on the literature that is more closely related to this thesis and the discussion that has influenced the development of the thesis. Some sources will be briefly discussed or will highlight only the aspects that directly relate to this thesis.

The works of Chiu[100] and Johnson[101] provide thought provoking monographs that primarily focus on cryptoassets and suggest the need for a new and more informed regulatory approach within this field. Both works will be referenced throughout, but the broader work of Chiu will provide the basis of the discussion around choices of policy in respect to the regulatory approach within the UK, as protection of users who might suffer loss because of failures in unpermissioned blockchains would be one approach to addressing the lack of legal redress. Chiu highlights the range of policy choices available in the context of cryptoasset regulation; frames the current legal approach within the UK; and the unlikelihood that such a regulatory approach will alter significantly in the coming years.[102] The work of Chiu advances the literature and will be utilised in the context of framing the current approach as well as some alternative approaches available. It can also be distinguished clearly here as this thesis will focus on the perspective of the end users where possible rather than purely the regulator.

[100] Iris Chiu, *Regulating the Crypto Economy Business Transformations and Financialisation* (Hart Publishing 2021).
[101] Syren Johnstone, *Rethinking the Regulation of Cryptoassets: Cryptographic Consensus Technology and the New Prospect* (Elgar Publishing 2021).
[102] Chiu (n 100), Pages 263-264.

Additionally, by raising the different methods of transaction as a key distinction to explore and by analysing the possibility of self-management within the peer-to-peer method, this thesis will further distinguish itself from the work of Chiu.

Walch[103] has suggested the significance of the presence of coders within blockchain and this will help to shape the discussions on liability throughout. This ties in well with the concept of "code as law" which will be referenced throughout.[104] The emphasis placed on coders in Walch's work raises the issue of whether any form of liability can be attached to coders themselves, which has already been identified as lacking a clear hierarchy in section 1.3.1 and will be developed further throughout the thesis. Building on this point, there will be the exploration of the best possible solution for the end user should systematic errors cause losses within unpermissioned blockchain technology.

A key influence in the development of this thesis was the work of Zetzsche, Buckley and Arner[105] who provide a thorough analysis of liability issues within unpermissioned blockchain technology as well as some obstacles from the regulator's perspective. These obstacles will be explored further in sections 2.3 and 2.4 respectively. One significant acknowledgment is that traditional legal frameworks seem to be incompatible with DLT.[106] This is a key aspect for this thesis as there will be the

[103] Walch (n 81).
[104] For further discussion on this concept see, Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books 2006); Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999); Karen Yeung, 'Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law' (2019) 82 (2) The Modern Law Review 207; Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> Accessed 1st February 2023; Katrin Becker, 'Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries' (2022) 33 Law Critique 113; Sai Agnikhotram and Antonios Kouroutakis, 'Doctrinal Challenges for the Legality of Smart Contracts: Lex Cryptographia or a New, Smart Way to Contract' (2019) 19 Journal of High Technology Law 300; Michael Schillig, 'Lex Cryptographi(c)a, Cloud Crypto Land or What? – Blockchain Technology on the Legal Hype Cycle' (2023) 86(1) Modern Law Review 31.
[105] Dirk Zetzsche, Ross Buckley and Douglas Arner, 'The Distributed Liability of Distributed Ledgers: Legal risks of Blockchain' (2018) University of Illinois Law Review 1361.
[106] Ibid, Page 1388.

analysis of whether unpermissioned blockchain technology more specifically is incompatible with traditional legal frameworks. The Zetzsche, Buckley and Arner article advances the literature regarding DLT more broadly by discussing liability issues and obstacles but does so through the application of general principles of law[107] and focuses on the perspective of the regulator. [108] This thesis will therefore provide an analysis of English law and primarily focus on the perspectives of the end users within unpermissioned blockchain technology.[109]

Another work that influenced the project, particularly in the early stages, is a paper by Tendon and Ganado.[110] The key aspect proposed by them is supporting the notion of the creation of a legal personality of blockchain technology.[111] This legal personality could potentially be attached to Decentralised Autonomous Organisations (hereby DAOs). A cryptocurrency such as Bitcoin could potentially be operated via a DAO, as the governance of the system relies upon the open-source coding in the medium of "cryptographic proof".[112] This theme of legal personality and DAOs do not feature prominently in this thesis, which considers the liability of individuals to a greater extent.

The final source that is worth mentioning in the framing of the project is the Financial Conduct Authority's (FCA) guidance paper on cryptoassets.[113] This paper clearly lays out the regulatory approach to cryptoassets hitherto adopted within the UK.

---

[107] Ibid, Page 1366.
[108] For more information on some of the regulatory concerns see Zetzsche, Buckley and Arner (n 105).
[109] It can be mentioned that other articles have dealt with a specific legal analysis but have covered other topics. For Blockchain and Copyright see Balazs Bodo, Daniel Gervais and Joao Pedro Quintais, 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26 (4) International Journal of Law and Information Technology 311). From a money laundering perspective see Houben (n 60).
[110] Steve Tendon and Max Ganado, 'Legal Personality for Blockchains, DAOs and Smart Contracts' (2018) 1 Corporate Finance and Capital Markets Law Review 1.
[111] Ibid, Page 2.
[112] Nakamoto (n 51), Page 1.
[113] Financial Conduct Authority, 'Guidance on Cryptoassets: Consultation Paper CP19/3' (FCA CP19/3 2019) <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> Accessed 1st February 2023.

In the context of liability for systematic errors, this approach is one which primarily focuses on warning users of the risks present within the market and that there is minimal legal protection afforded to the end users in the event of loss.[114] The Taskforce also sets out its concern that many individuals do not have the required knowledge to operate in such a risky field.[115] The FCA reference the volatility of cryptocurrency such as Bitcoin[116] and the decentralised nature of the underlying technology as key reasons for the lack of legal intervention.[117] The volatility of the asset renders it difficult to regulate in line with traditional fiat currencies and the decentralised nature creates a key barrier to the determination of legal liability and who should be responsible. This guidance paper approaches from an economic perspective which further justifies the lack of legal protection. Largely this is because presently cryptocurrencies do not pose a viable threat to fiat currencies which can limit the need for legal intervention.[118] This paper is important as it covers many aspects which have been the key components of the current approach to regulation of cryptoassets more generally in the UK. Whilst this is the present position, the Taskforce also make it one of their objectives "to secure an appropriate degree of protection for consumers"[119] and as this thesis was nearing completion a consultation on regulation was launched.

In this consultation, there is the acknowledgement of the speedy and complex nature in which the cryptoasset markets are developing as well as a recognition that risk

[114] Ibid, Page 12.
[115] Ibid, Page 11; There is even the suggestion that users may "overestimate their knowledge of cryptoassets". This also supports a wider view in England as the Bank of England view cryptocurrencies as an illogical investment strategy. For further information see, Bank of England, 'Digital Currencies' (5th March 2019) <https://www.bankofengland.co.uk/research/digital-currencies> Accessed 1st February 2023.
[116] Financial Conduct Authority (n 113), Page 9.
[117] Ibid, Page 23.
[118] Bank of England Financial Policy Committee, 'Financial Policy Committee Statement from its policy meeting 12 March 2018' (FPC 2018) <https://www.bankofengland.co.uk/-/media/boe/files/statement/fpc/2018/financial-policy-committee-statement-march-2018.pdf?la=en&hash=61059A79F4453B2EFA6BA88A598739DD67FC0CD7> Accessed 1st February 2023, Page 2.
[119] Financial Conduct Authority (n 113), Page 16.

must be managed without stifling innovation.[120] The consultation also notes a rise in usage with "5-10% of UK adults" now owning cryptoasset and institutional bodies engaging more in the field.[121] Although it appears that the current approach will largely revolve around warning users of risk to ensure that they can operate in an informed manner,[122] there is also the understanding that the regulatory approach is one that must be flexible and may require different regulatory approaches as the market and usage of the technology continues to develop.[123] Furthermore, there is some clarity provided regarding the location of the activity and whether it falls within the UK regulatory parameters. Effectively, where the cryptoasset provider or customer are in the UK then generally it will be within the scope of regulated activities.[124] The consultation paper primarily provides a series of broadly mapped out possibilities for the regulatory landscape of the future without seeking to alter the current regulatory landscape significantly.

It is also worth noting that some of the literature focuses on the way the technology works and what benefits or issues could arise,[125] including the practical usage of DLT for the financial industry.[126] Although these academic technical papers are important for providing a deep technical understanding of the operation of

[120] HM Treasury, 'Future financial services regulatory regime for cryptoasset: Consultation and call for evidence' (February 2023) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf> Accessed 1st February 2023, Page 5.
[121] Ibid, Pages 8-9.
[122] Ibid, Pages 18-20.
[123] Ibid, Pages 10-11.
[124] Ibid, Pages 24-25.
[125] A good example of this is Melanie Swan, *Blockchain: Blueprint for a New Economy* (O'Reilly 2015). Other examples can include Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1 which focuses on issues of an exchange-based system or Olivier Hari and Ulysse Pasquier, 'Blockchain and distributed ledger technology (DLT): academic overview of the technical and legal framework and challenges for lawyers' (2018) 5 International Business Law Journal 423 which explains how DLT works in order to explain the legal issues that could arise.
[126] The best example of this is Hong Kong Monetary Authority (n 12).

unpermissioned blockchain technology, they do not focus on the legal aspect and so were not key sources for thesis.[127]

1.5: Original contribution

This thesis seeks primarily to establish that a lack of legal redress through contract and tort in English law for systematic errors within unpermissioned blockchain technology is present. Furthermore, there will be the determination of whether the current level of risk warrants legal redress. This will be considered as one of the factors that might justify command-and-control regulation within the peer-to-peer method. Additionally, regulation will be assessed in a decentred manner, using Ostrom's self-management principles to determine if self-regulation would be an appropriate form of governance.[128] This will advance the knowledge within the field and will provide a key work to be further critiqued.

More specifically this thesis will address three hitherto under-researched aspects. Firstly, by applying contract and tort law based on the English legal system to liability issues arising out of systematic errors within unpermissioned blockchain technology in the context of peer-to-peer transactions, the current level of legal protection will be explored. Furthermore, there will be the discussion of the practical difficulties any party who is seeking redress for loss suffered because of fault is likely to face, due to the decentralised nature of the technology and the potential anonymity of users and fraudsters.[129]

[127] For the focus of this legal research, the operation of unpermissioned blockchain technology has been adequately covered in section 1.1 and any security aspects will be covered in section 2.4. However, for an example of a more detailed explanation of the operation of unpermissioned blockchain technology see Hong Kong Monetary Authority (n 12).

[128] For a discussion of Ostrom's self-management principle in blockchain and some changes to the blockchain governance structure that could aid a platform in self-managing see, Sangita Gazi and others, 'Blockchain as Commons: Applying Ostrom's Polycentric Approach to Blockchain Governance' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4250547> Accessed 1st August 2023.

[129] For a brief discussion of how unpermissioned blockchain technology makes no reference to any hierarchy see, Hong Kong Monetary Authority (n 66), Page 104.

The second contribution to knowledge will be the application of Ostrom's self-management theory to unpermissioned blockchain technology in the peer-to-peer context. Ostrom's approach of self-management or self-regulation is potentially a practical governance system within the peer-to-peer method of transaction.[130] The third contribution will be reached by providing recommendations for the regulatory landscape moving forward and specifying that the main focus for regulation should be at the point where the public are exposed to unpermissioned blockchain technology, namely through cryptocurrency exchanges, including DEX.

In summary, the key contributions of this thesis may suggest that regulatory attention should be paid to the risk of systematic errors within unpermissioned blockchain technology and the potential liability issues that could arise. Moving forward, this thesis can provide insight into the types of risks that are present, current potential for redress in contract and tort, the importance of distinguishing between different forms of blockchain and their methods of transaction, and the recommended regulatory approaches.[131] This thesis will provide a clear framework which can be flexible to the evolution[132] that is coming.[133]

---

[130] Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press 1990); Elinor Ostrom, 'Tragedy of the Commons', in Steven N Durlauf and Lawrence E Blume (ed) *The New Palgrave Dictionary of Economics* (2nd edn Palgrave Macmillan 2008); For an interesting discussion on 'self-management' within decentralised platforms see, Chiu (n 100), Pages 295-297 and also pages 262, 280, 284 and 288.

[131] For further discussion of some of these developing and changing approaches see, Bronwyn Howell and Petrus Potgieter, 'Regulating Cryptocurrencies: mapping economic objectives and technological feasibilities' (September 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3927658> Accessed 1st February 2023, Pages 9-11.

[132] For some examples of how the landscape may change in coming years see, Andreas Bogner, Mathieu Chanson and Arne Meeuw, 'A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain' IoT'16: Proceedings of the 6th International Conference on the Internet of Things (November 2016) 177 <https://doi.org/10.1145/2991561.2998465> Accessed 1st February 2023; Foteni Valeonti and others, 'Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs)' (2021) 11 Applied Sciences 9931 <https://www.mdpi.com/2076-3417/11/21/9931#cite> Accessed 1st February 2023; Maria Demertzis, 'Non-fungible tokens (NFTs): The next chapter in crypto' (January 2022) Bruegel-Blogs <https://go.gale.com/ps/i.do?id=GALE%7CA690531927&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=&p=AONE&sw=w&userGroupName=anon%7Ed2a2fd82> Accessed 1st February 2023; TheTruthDrops, 'World Government Summit 2022: Dr Pippa Malmgren Talks About Blockchain & Digital Currencies' (2nd April 2022) <https://www.youtube.com/watch?v=cvXdSvja-aI> Accessed 1st February 2023.

[133] Howell and Potgieter (n 131), Pages 11-12.

1.6: Why focus on unpermissioned blockchain technology?

From the literature, it appears that some new technologies may not clearly fit traditional ways of contracting. Therefore, this thesis will focus on unpermissioned blockchain technology to consider how a novel technology can still be addressed by the law in England and Wales. This legal analysis of unpermissioned blockchain technology will use Bitcoin as a key example, on which there is plenty of literature[134] and complexities to be addressed.[135]

As well as this, there is the possibility to assess the methods of transaction within unpermissioned blockchain technology and determine whether the regulatory landscape across such methods should be fundamentally distinct from one another. As a result, this thesis will seek a best-case solution for liability issues arising from systematic errors in unpermissioned blockchain technology. There is also the scope to provide general recommendations for legal issues that can arise broadly within DLT and therefore, blockchain.

This is a vital aspect for the thesis as it anticipates that the technology itself will continue to develop and there may be increased use by the general public.[136] At that point a need for greater regulation might arise to address risks such as errors in the underlying blockchain. However, due to the lack of a requirement for a central party

---

[134] Fred Cate and others, 'Blockchain versus data-protection' (2018) 8(2) International Data Privacy Law 103, Page 103.

[135] UK Jurisdiction Taskforce, 'Legal statement on cryptoassets and smart contracts' (The LawTech Delivery Panel) <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.lawgazette.co.uk%2Fcommentary-and-opinion%2Fcrypto-law-still-has-known-unknowns%2F5102223.article&data=01%7C01%7Caki.elmenshawy2014%40my.ntu.ac.uk%7Cefb8a9bf0b174b638aa508d76e9e77dc%7C8acbc2c5c8ed42c78169ba438a0dbe2f%7C0&sdata=vHbPiEGhadPlL6gWdBSgBhGOHE3uBavzGk%2BN4i%2B1xwQ%3D&reserved=0> Accessed 1st February 2023, Pages 6 & 9-10; UK Jurisdiction Taskforce, 'The Launch of the Legal Statement on the Statues of Cryptoassets and Smart Contracts' (November 2019) <https://www.judiciary.uk/wp-content/uploads/2019/11/LegalStatementLaunch.GV_.2-1.pdf > Accessed 1st February 2023.

[136] For an example of how this area is constantly changing, at the outset of the thesis, Libra was regarded as a permissioned blockchain cryptocurrency that could revolutionise the industry but instead was unsuccessful. For further discussion of Libra, see Libra.org, 'The Libra Blockchain' <https://developers.libra.org/docs/the-libra-blockchain-paper> Accessed 1st February 2023.

within unpermissioned blockchain technology, the main threat or main potential, depending how it is viewed is that it could enable a challenging of the central powers of traditional finance, and consumer protections that are built into that sector are bypassed.[137] As a result, the uncertainty of legal redress within unpermissioned blockchain technology renders it an important discussion within the legal field and provides a key reason for this thesis focusing on unpermissioned blockchain technology.

Having established gaps in the literature and therefore, reasons why unpermissioned blockchain technology is a focus of this research, the overall research question can now be explained with greater clarity.

1.7: Research Question

The research question centres itself around the potential for legal redress for systematic errors within unpermissioned blockchain technology, in accordance with English law. This means ultimately that two questions will be answered throughout the course of the thesis. Firstly, is legal redress for systematic errors within unpermissioned blockchain technology possible, and secondly, would such legal redress be considered necessary. These questions shall be answered primarily through a doctrinal study of the existing English legal framework, including some discussion of contractual liability, but primarily relating to noncontractual liability. Focusing principally on the English legal framework provides a solution to the issue that there is currently limited case law in respect of contract and tort as the main possible avenues for redress in the event of fault. The *Tulip Trading* case,[138] which has now progressed to the Court of Appeal,[139]

[137] For further discussion on this see, Marcella Atzori, 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' (2017) 6(1) Journal of Governance and Regulation 45.
[138] *Tulip Trading Ltd* v *Bitcoin Association for BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624.
[139] *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16.

provides one of the only cases thus far in this area but the issues itself were not discussed in detail.

Given the risk to the public presented by unpermissioned blockchain and the risk for errors, broader regulatory issues are considered. As a way to approach regulatory issues without undermining the nature of unpermissioned blockchains the analytical approaches of the self-management principles according to Ostrom[140] and the theory of regulation will enhance the findings in relation to the central questions.

To answer these central questions, this thesis can be viewed in three stages. First is the general discussion of risks. Second is an exploration of who ought to be liable. Following this will be the analysis of whether there is likely to be redress under English law in contract and tort. Furthermore, it will be assessed as to whether this lack of redress, alongside other risks, presents a case for regulation, using a framework of decentred regulation. Finally, since a lack of likely redress for errors in unpermissioned blockchains is unlikely to be available, but it does not in itself present a case for greater formal regulation, there will be the analysis of how Ostrom's work can be used to structure a system of self-regulation under a decentred approach, with a view to responsibility for errors being allocated under that approach.

Determining the most suitable form of legal redress for systematic faults within unpermissioned blockchain technology will require a broad analysis. Consequently, that is why this thesis began with establishing the context of the technology. This useful basis of knowledge from an operational and practical perspective will aid the development of the analysis throughout this thesis. The project in Chapter 2 will then

[140] Elinor Ostrom, 'Coping with Tragedies of the Commons' (1999) 2 Annual Review of Political Science 493.

focus on the variety of risks that occur within unpermissioned blockchain technology.[141] The primary focus of Chapter 2 shall be to highlight a variety of concerns from a user's perspective as well as the practical obstacles that any litigant would face.

There will then follow a theoretical analysis of where liability for faults should lie, which builds upon the exploration of any proposed hierarchy of responsibility within unpermissioned blockchain technology.[142] The thesis will seek to analyse whether there is a differing approach that may be required to adequately deal with the divergence of a platform using unpermissioned blockchain technology such as Bitcoin, from a truly peer-to-peer network, to one which has been made accessible to the public through the intermediary of exchanges and whether, alongside other risks, this presents a case for greater regulation. The discussion of regulation theory, will primarily focus on whether a justification for regulation within this context, exists. This will help to answer the central questions as justifying regulation is a necessary component of enabling legal redress to be achieved. Contrary to this, if regulation cannot be justified then it may suggest that legal redress is not necessary in this context and possibilities for self-regulation will be explored. This analysis will ultimately help to determine what the best solution is for systematic errors within unpermissioned blockchain technology which will provide an answer to both central questions for this thesis.

In pursuing this research there are three key objectives.

- To discuss the risks present within unpermissioned blockchain technology to understand where faults may arise for which users may seek redress.

[141] Dirk Zetzsche, Ross Buckley and Douglas Arner, The Distributed Liability of Distributed Ledgers: Legal risks of Blockchain (2018) University of Illinois Law Review 1361.
[142] Ibid, Page 1384.

- To analyse whether the current traditional avenues of contract and tort provide practical redress for end users who suffer loss from systematic errors within unpermissioned blockchain technology.

- To determine when regulation for systematic errors may be justified in the context of unpermissioned blockchain technology and explore the range of regulatory options on a risk-based approach, considering the contexts in which the general public may encounter usage of unpermissioned blockchains.

1.8: Methodology

The foundation of the project is comprised of the doctrinal and theoretical elements. The primary method is doctrinal, which is common in the legal sphere[143] to "identify, analyse and synthesise the context of the law."[144] Historically, any form of legal scholarship primarily focused on the law itself, societal problems and the law's interaction with society.[145] In this respect, this thesis follows the traditional form of legal scholarship with analysis of the law and its current potential interaction with unpermissioned blockchain technology. Chapter 4 will follow a traditional doctrinal approach, with analysis of the black letter law and the "use (of) interpretative tools or legal reasoning to evaluate legal rules and suggest recommendations for further development of the law."[146] The purpose of this will be to determine whether English

[143] Laura Cahillane and Jennifer Schweppe, *Legal Research Methods: Principles and Practicalities* (Clarus Press 2016), Page 3.
[144] Terry Hutchinson, 'Chapter 1: Doctrinal Research' in Dawn Watkins and Mandy Burton (ed), *Research Methods in Law* (2nd edn, Routledge 2017), Page 13.
[145] Mike McConville and Wing Hong Chui, *Research Methods for Law* (2nd edn, Edinburgh University Press 2017), Page 1.
[146] Ibid, Page 4. Whilst the doctrinal approach is sometimes believed to be a simplistic approach, it is "complex, multi-layered, and distinctive" (Cahillane and Schweppe (n 143), Page 21). Some could even argue that the doctrinal approach shows a closer resemblance to "methodology of other disciplines" (Mark Van Hoeke, *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Bloomsbury 2011), Page 11; Hutchinson (n 144), Pages 17-18).

law potentially sufficiently protects users in terms of liability for systematic risks within unpermissioned blockchain technology.[147]

The doctrinal study of the existing law will be supplemented and framed primarily around regulation theory.[148] Analysing the potential justification of regulation within unpermissioned blockchain technology will be essential to determine whether regulation under a decentred approach could be a valid approach in the context of liability issues arising from systematic errors. As part of this decentred approach, Ostrom's self-management theory will be applied to unpermissioned blockchain technology to understand whether theoretically the system may be better suited to self-regulation.

1.9: Structure of the thesis

As mentioned previously, Chapter 2 will focus on the risks present within unpermissioned blockchain technology which could give rise to claims for liability for fault and the key obstacles such as anonymity and jurisdictional problems that may provide a barrier to legal redress.[149] Chapter 3 builds on the discussion in section 1.3.1 by discussing the theoretical underpinning of liability and its application to unpermissioned blockchain technology. Chapter 4 will then explore the doctrinal legal framework under English Law, primarily focusing on contract and tort law as potential strands of law for users seeking legal redress for systematic errors. In Chapter 5, potential policy choices for regulators will be considered to assess the possibility of

[147] At the time of beginning this research, there was no discussion of this specific matter in any of the literature.
[148] This two-strand study, covering the doctrinal legal and theoretical elements is not uncommon in the legal sphere, and would be regarded as largely traditional. See McConville and Chui (n 145), Page 20. This is due to the analysis of the legal framework, including relevant legislation and case law, and the analysis of doctrinal literature. See Philip Langbroek and others, 'Methodology of Legal Research: Challenges and Opportunities' (2017) 13 (3) Utrecht Law Review, Page 2.
[149] Houben (n 60), Pages 263-264; Olivier Hari and Ulysse Pasquier, 'Blockchain and distributed ledger technology (DLT): academic overview of the technical and legal framework and challenges for lawyers' (2018) 5 International Business Law Journal 423, Page 444.

greater protection for users within unpermissioned blockchain technology.[150] This will be framed around the assessment of the applicability of decentred regulation[151] and the consideration of risk as a possible justification of regulation.[152] To analyse the potential for self-regulation within the peer-to-peer method Ostrom's self-management theory will be applied. Chapter 6 will then suggest 6 key recommendations for the regulatory landscape moving forward. Finally, Chapter 7 will provide a conclusion to this thesis and a determination of whether legal redress is possible and necessary for systematic errors within unpermissioned blockchain technology.

The law is stated as at 31 January 2023 although where possible account has been taken of later developments.

[150] Chiu (n 100), Pages 263-271.
[151] Julia Black, 'The Role of Risk in Regulatory Processes' in Robert Baldwin, Martin Cave and Martin Lodge (ed), *The Oxford Handbook of Regulation* (Oxford University Press 2010).
[152] Ibid.

Chapter 2: Mapping Existing Risks and Obstacles to Legal Redress within Unpermissioned Blockchain Technology

2.1: Introduction

To inform the central question of whether legal redress is possible for systematic errors within unpermissioned blockchain technology, a greater understanding of the broader risks and obstacles of this technology is needed. The nature of unpermissioned blockchain technology, having evolved in an anti-establishment manner,[153] raises the question of whether it can ever be reconciled with existing law. This chapter will highlight the existing risks and obstacles to enforcement of claims that could prevent compatibility with current legal frameworks.

This chapter shall proceed by first exploring three key risks within unpermissioned blockchain technology, that may give rise to loss for the end user. The first risk highlighted will discuss the potential coding errors that may be present in the underlying blockchain. The second risk highlighted and arguably the most prominently discussed risk currently is the risk of hacking or coding errors within the system.[154] Unpermissioned blockchain technology, although often praised due to its secure nature and immutability, it is still vulnerable to hacks and this is the case for different methods of transaction that end users utilise:[155] the verification processes of the blockchain can be undermined, an exchange can be hacked or DeFi transaction can be hacked. The

[153] Amelia Schwanke, 'Bridging the digital gap: How tax fits into cryptocurrencies and blockchain development' (2017) 28 International Tax Review 20, Page 21; Erika Strebel, 'Caution is key with cryptocurrency' (2018) Wisconsin Law Journal, Page 2; Phil Ariss, 'Money for Nothing?' (2017) Credit Management 13 <https://search.proquest.com/docview/1963932998?rfr_id=info%3Axri%2Fsid%3Aprimo&accountid=1469> Accessed 1st February 2023, Page 14. An adapted version of the discussion in this chapter forms the basis for one of my published papers, although some of the sections are identical see, Akrum El Menshawy, 'Mapping Existing Risks and Obstacles to Legal Redress Within Unpermissioned Blockchain Technology' (2022) 10 NIBLeJ 6.

[154] See section 2.4.

[155] Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1, Pages 1-5; Nakamoto (n 51); Financial Conduct Authority (n 113), Page 12.

third key risk that will be explored is the possibility of collusion of miners, which has potential due to the presence of mining pools.

Following on from the discussion of these key risks, the two main obstacles to legal redress will be explored in the form of anonymity and jurisdictional complications. Regarding anonymity, this is a particularly prevalent issue at the root of unpermissioned blockchain technology.[156] Any litigant who suffers loss because of a fault in the unpermissioned blockchain will find that anonymity is a problem. Also, from a regulatory perspective, this is a pressing concern as anonymity is an obstacle that will prevent enforcement of regulation.[157] If enforcement of regulation is difficult, then the regulation itself is diminished and less effective.

Regarding the second obstacle of jurisdictional complications, this may be deemed a significant obstacle to legal redress because of unpermissioned blockchain technology being a supranational technology[158] which give rise to issues of applicable and governing law. For this thesis, the "supranational" nature of the technology refers to the idea that a decentralised information ledger with the potential for anonymity enables unpermissioned blockchain technology's operation to transcend clearly defined jurisdictions. It has the potential to be located everywhere due to user interaction but also does not necessarily have a defined location of origin. The combination of the supranational nature of the technology and the potential anonymity of coders, miners and peer-to-peer end users presents significant obstacles to legal redress for systematic errors within unpermissioned blockchain technology, as well as potentially presenting

[156] One which is being discussed by many jurisdictions. For a particular example relating to anonymity and GDPR within the EU, see Dr Michele Finck (STOA), 'Blockchain and the General Data Protection Regulation' (2019) PE 643.445 July, <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf > Accessed 1st February 2023.

[157] The problem of anonymity operating within cyberspace has been a subject for debate since the formation of cyberspace itself. For some discussion of this see Jonathan Edelstein, 'Anonymity and international law Enforcement in Cyberspace' (1996) Autumn (1) Fordham Intellectual Property, Media & Entertainment Law Journal 231.

[158] Bjelajac and Bajac (n 54), Page 22.

wider regulatory difficulties. Both obstacles of anonymity and of uncertain jurisdiction will be referenced throughout the thesis when considering the practicality of legal redress. Additionally, this chapter will briefly explore political aspects, as well as factors of privacy, criminal activity and environment costs as issues within the field more broadly that may, alongside the risk of a lack of redress for faults, present a level of risk justifying regulation.

2.1.1: Overview of Unpermissioned Blockchain Risk

Blockchain technology may be said to have developed an aura of perfection amongst users, often referenced as the immutability of blockchain.[159] This concept of "immutability" refers to the permanence of the ledger and the fact it cannot be altered.[160] The permanence of the ledger may be a vital principle of blockchain technology, but it also leads users to believe that there is no risk of hacking.[161] Despite this perception of safety amongst users, regulators warn of the risks associated with cryptocurrencies that use blockchain technology.[162] The Financial Conduct Authority has even stated that users may "overestimate their knowledge of cryptoassets [that use blockchain technology]".[163] Potentially users are therefore misinformed in their belief that all forms of interaction with blockchain technology are protected against certain risks due to the immutability.

[159] Roberto Domingos Taufik, 'Block Change: The Fallacy of Blockchain Immutability and Cartel Governance' (2020) 1 Notre Dame Journal on Emerging technologies 307, Page 315. The definition of immutable is "not changing, or unable to be changed" see Cambridge Dictionary, 'Immutable' (2023) <https://dictionary.cambridge.org/dictionary/english/immutable> Accessed 1st February 2023.
[160] Roberto Domingos Taufik, 'Block Change: The Fallacy of Blockchain Immutability and Cartel Governance' (2020) 1 Notre Dame Journal on Emerging technologies 307, Page 311; Hong Kong Monetary Authority (n 12), Page 16.
[161] Financial Conduct Authority (n 113), Page 12. Hacking is used in a broad manner in this context.
[162] Ibid, Page 11.
[163] Ibid.

Blockchain technology has wide-ranging potential applicability,[164] yet as usage increases, so does the potential for risks and threats to the notion of immutability. Renn defines risk as "the possibility that human actions or events lead to consequences that affect aspects of what humans value".[165] Renn suggests that humans understand the connection between actions and consequences and there is a desire "to reduce undesirable effects through appropriate modification of the causes or, through less desirable, mitigation of the consequences."[166] This notion of risk is capable of application within the field of technology.[167] In this chapter, the "risk" discussed will primarily focus on the possibility for coding errors and collusion. By stating the obstacles to legal redress, this chapter will highlight barriers to legal mitigation of the consequences of these risks.

Some of the risks within the cryptocurrency market, as an example, have seemingly been accepted by the end users. For example, it has been suggested that Bitcoin peer-to-peer users do acknowledge the high volatility within the market and the lack of legal protection.[168] However, this suggestion was made in 2013 and there were significantly fewer exchanges at the time. Therefore, peer-to-peer users may have been more knowledgeable in the technology itself as they would have more likely been miners and coders. More recently, there has appeared to be a rather nonchalant approach from exchange customers to risks within the cryptocurrency market specifically. Exchange customers seem to accept that there is a high risk, but they are willing to

[164] For an insight into potential sectors that could adopt blockchain see, cbinsights.com, 'Banking is only the beginning: 58 big industries Blockchain could transform' (March 2021) <https://www.cbinsights.com/research/industries-disrupted-blockchain/> Accessed 1st February 2023.
[165] Ortwin Renn, 'Three Decades of Risk Research: Accomplishments and New Challenges' (1998) 1 Journal of Risk Research 49, Page 51.
[166] Ibid.
[167] For an example of how this can be applied in cloud computing see, Rebecca Parry and Roger Bisson, 'Legal approaches to management of the risks of cloud computing insolvencies' (2020) Journal of Corporate Law Studies 1, Page 4.
[168] Variale (n 53), Page 18.

engage with it nonetheless due to the potential for high rewards.[169] The same could be true of DEX customers also. Although such customers may become more wary following recent high-profile instances such as the failures of the FTX exchange and stablecoin Terra/Luna.[170]

However, in relation to the awareness of risks some argue that "a large proportion of society does not yet understand what blockchains or cryptocurrencies are or how they can use them"[171] and therefore, could not be aware of the risks of the technology when they have no understanding of the technology itself. Therefore, this chapter will provide a clear insight into the types of risk present and the obstacles to legal redress with later chapters presenting a more detailed examination of one of these risks, namely faults in the blockchain. This will inform the discussion throughout the thesis as to what risks may warrant further legal protection and the obstacles that must be overcome to better protect end users.

2.2: Security Aspects of Risk Mitigation

Prior to understanding the some of the key risks present, we must first recognise the safeguards that may give an impression of protection from risk. The use of cryptography is a vital component of the immutability of unpermissioned blockchain technology. In a platform that uses unpermissioned blockchain technology, the private cryptographic key is essential to ensure that the party receiving the property is the

[169] For more information see Financial Conduct Authority, 'How and why consumers buy cryptoassets: a report for the FCA' (FCA October 2018) <https://www.fca.org.uk/publication/research/how-and-why-consumers-buy-cryptoassets.pdf> Accessed 1st February 2023, Page 14.
[170] For a discussion on FTX see, George Calhoun (forbes.com), 'FTX and ESG: A Panorama of Failed Governance (Pt 1 – The Internal Failures)' (November 2022) <https://www.forbes.com/sites/georgecalhoun/2022/11/21/ftx-and-esg-a-panorama-of-failed-governance-pt-1--the-internal-failures/> Accessed 1st February 2023. For a discussion on Terra/Luna see, Q.ai (forbes.com), 'What Really Happened To LUNA Crypto' (September 2022) <https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=68ff269a4ff1> Accessed 1st February 2023.
[171] Alex Hughes and others, 'Beyond Bitcoin: What blockchain and distributed ledger technologies means for firms' (2018) Business Horizons 1551 1, Page 7.

intended party.[172] A private key can be defined as the decryption key, whereas the public key is the encryption key. Therefore, if *A* wishes to transfer property to *B* through cryptography, then *A* will send the property to *B's* public key. Anyone can send property to the public key as it is public. The public key will then encrypt the property transferred, meaning that only *B's* private key can decrypt it to view or access the property. Hughes, Park, Kietzmann and Archer-Brown state that "Parties that wish to take part in a transaction do not even need to know each other's identities, but they can be assured that the intended party is the sender/receiver since only the intended party has access to his/her own private key".[173] The threat of this private key being stolen will be discussed later in this chapter.

Additionally, the unique hash code created for each addition or alteration to the platform is another aspect of the security of unpermissioned blockchain technology.[174] Every transaction on the blockchain has its own unique and random hash code. This unpredictability helps to ensure the security of unpermissioned blockchain technology. Every change or addition to a platform not only forms a unique and unpredictable hash code but is bound with the previous information added to the blockchain.[175] The hash code of the new block in unpermissioned blockchain technology will bind itself to the hash code of the previous block, and so forth. For example, if *A* transfers an asset to *B*, a unique hash code will be created once this transaction is validated. When *B* then goes to transfer that asset to *C*, another unique hash code will be created. As part of the validation process, the miners will ensure that the new hash code is bound to the

[172] "The two basic infrastructures used in cryptographic systems are public-key and private-key. While early computer systems used private-key cryptography almost exclusively, by the late 1990s and early 2000s the tide was shifting in favor of public-key cryptography." See encyclopedia.com, 'Cryptography, Public and Private Key' 16th March 2020 <https://www.encyclopedia.com/economics/encyclopedias-almanacs-transcripts-and-maps/cryptography-public-and-private-key> Accessed 1st February 2023.
[173] Hughes and others (n 171), Page 4.
[174] It may even be regarded as the most pivotal aspect to the security of any platform using unpermissioned blockchain technology. See Hong Kong Monetary Authority (n 12), Page 16.
[175] Ibid, Page 5.

previous one. This is not done by a literal investigation by the miners but by running the software for the calculations; the software automatically checks the validity of the hash code. If a block is not bound to the previous one then it means it is not a valid transaction.[176] As a result, it makes "unauthorised changes… very difficult, if not impossible."[177] For a visual representation of how the hash code can develop please see figure 2 below.

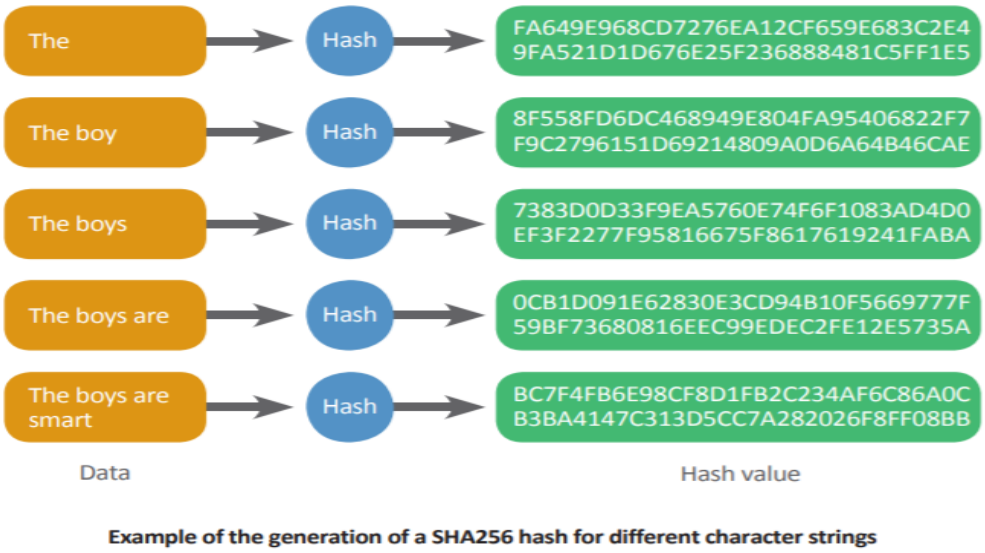

Figure 2: Hash code example (HKMA 2016 Whitepaper on Distributed Ledger Technology 1.0)[178]

Figure 2 shows that with each new entry of data within an unpermissioned blockchain, a hash code is randomly generated which affects the hash value. This aids the concept of immutability as not only are the blocks permanent but an individual would not be able to add a false block to the blockchain as there is no feasible way of

[176] For a discussion of this in the context of a blockchain based voting system see, Divya K and Usha K, 'Blockvoting: An Online Voting System Using Block Chain' (2022) International Conference on Innovative Trends in Information Technology (ICITIIT) (February 2022) <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9744132> Accessed 1st February 2023, Para II. For a discussion of this in the context of smart cities see, Rizwan Patan and others, 'Blockchain Security Using Merkle Hash Zero Correlation Distinguisher for the IoT in Smart Cities' (2022) 9(19) IEEE Internet of Things Journal 19296, Section V.
[177] Hong Kong Monetary Authority (n 12), Page 5.
[178] Source: Ibid, Page 23.

being able to predict how the hash code would be randomly generated for each new block.[179] Whilst there is the possibility that the hash could be broken by brute force, which would involve a programme running that would try different passwords until the correct one was identified, this is highly difficult providing the hash-function used is secure.[180]

Another key element to the immutability of unpermissioned blockchain technology is proof-of-work as it is a key component to validation.[181] Proof-of-work seems to be the most used method of validation within unpermissioned blockchain technology.[182] More recently there is the introduction of proof-of-stake as an alternative to proof-of-work.[183] A detailed discussion of these protocols would not benefit this chapter.[184] The key aspect to highlight here is that such protocols exist to ensure a degree of security within unpermissioned blockchain technology. Proof-of-work is vital in unpermissioned blockchain technology as it provides for validation in place of a centralised party. Proof-of-work enables the validity to be secure and legitimate.[185] It includes the complex computerised algorithm that must be run for blocks to be added.[186] This intentionally slows down the validation process. In Bitcoin for example, proof-of-

[179] Alexander Savelyev, 'Copyright in the blockchain era: Promises and challenges' (2018) 34(3) Computer Law and Security Review 550, Page 554.
[180] Konstantinos Chalkias, Panagiotis Chatzigiannis and Yan Ji, 'Broken Proofs of Solvency in Blockchain Custodial Wallets and Exchanges' (2022) Paper 2022/043 Cryptology ePrint Archive <https://eprint.iacr.org/2022/043.pdf> Accessed 1st February 2023, Section 4.2; Shattered.io <https://shattered.io/> Accessed 1st February 2023.
[181] Savelyev (n 179), Page 559.
[182] BitFury Group, 'Proof of Stake versus Proof of Work White Paper 1.0' (2015) <https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf> Accessed 1st February 2023, Pages 5-6.
[183] Ibid, Pages 6-7. Proof-of-stake has significant benefits in respect of its environmental impact in comparison with the computational power required in Proof-of-work. For a discussion of how environmental regulation can impact innovation see, Jingxiao Zhang and others, 'The impact of environmental regulations on urban Green innovation efficiency: The case of Xi'an' (2020) 57 Sustainable Cities and Society, Article 102123.
[184] For more information on proof-of-stake see, Olivier Hari and Ulysse Pasquier, 'Blockchain and distributed ledger technology (DLT): academic overview of the technical and legal framework and challenges for lawyers' (2018) 5 International Business Law Journal 423, Page 427.
[185] Michael Nofer and others, 'Blockchain' (2017) 59(3) Business & Information Systems Engineering 183, Page 184.
[186] "*Proof-of-Work* implies that the miner has to resolve extremely complex mathematical problems that are also expensive in terms of energy consumption" see, Hari and Pasquier (n 184), Page 427.

work amounts to roughly ten minutes on average for the hashing power of the network to find a solution to the block hash and add a new block of transactions to the ledger.[187] This is regarded as an ideal balance in slowing the process down enough to validate accurately without making it impractical for transactions to take place.[188] Now that some of the key elements to the security of unpermissioned blockchain technology have been discussed, focus can be made on the key risks.

2.2.1: Coding errors

Although the above security aspects of risk mitigation exist, the underlying blockchain is capable of susceptibility to the threat of coding errors.[189] Several examples exist ranging from creating new Bitcoins via a coding error,[190] the Bitcoin update which was incompatible with the previous version[191] or the failure of the DAO.[192] The success of the security is heavily reliant on the underlying coding which can be susceptible to human error, thus resulting in the potential for coding errors. The importance of the underlying coding and the potential for issues to derive from the coding is recognised in the *Tulip Trading* case,[193] where the public nature of the blockchain and its source code created the possibility of the coding for the blockchain to

[187] Noureddine Lasla and others, 'Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm' (2022) 214 Computer Networks, Article 109118, Page 2; Simply Explained – Savjee, 'How does a blockchain work – Simply Explained' (2017) <https://www.youtube.com/watch?v=SSo_EIwHSd4> Accessed 1st February 2023, Minute 3:18-3:25.
[188] Pradip Kumar Sharma and Jong Hyuk Park, 'Blockchain based hybrid network architecture for the smart city' (2018) 86 Future Generation Computer Systems 650, Page 654.
[189] Md Rafiqul Islam and others, 'A Review on Blockchain Security Issues and Challenges' (2021) IEEE 12th Control and System Graduate Research Colloquium (ICSGRC) 227 <https://ieeexplore.ieee.org/abstract/document/9515276> Accessed 1st February 2023, Page 227.
[190] Matthew Zook and Joe Blankenship, 'New spaces of disruption? The failures of Bitcoin and the rhetorical power of algorithmic governance' (2018) 96 Geoforum 248, Page 251.
[191] For some discussion of this and several programming errors see, Fabio Lugano, 'Famous programming errors in the crypto world' (December 2018) <https://en.cryptonomist.ch/2018/12/08/programming-errors-crypto-world/> Accessed 1st February 2023.
[192] Brian Sanya Mondoh and others, 'Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion?' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144753> Accessed 1st February 2023; Peder Ostbye, 'Exploring The Role of Law in The Governance of Cryptocurrency Systems and Why Limited Liability DAOs might be a Bad Idea' (January 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007547> Accessed 1st February 2023.
[193] *Tulip Trading Ltd* v *Bitcoin Association for BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624; *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16.

be copied and the historic transactions to also be copied onto the new platform.[194] Further discussion of the examples of coding errors are not necessary. The key aspect to note is that evidence indicates they are a possibility.

2.2.2: Risk of Hacking

An additional key risk present is the potential for hacks across the various methods of transaction. Currently, as far as is known, all the reported hacks within the cryptocurrency sector have been hacks of the exchanges or DEXs and not direct hacks of the underlying blockchain.[195] As a result, it appears that the peer-to-peer method may be more enticing from a security perspective. The underlying blockchain in unpermissioned blockchain technology is considered immutable, however, it is important to note that the underlying blockchain is not 100% free of the potential to be hacked.[196]

Whilst a hack of the underlying blockchain is theoretically possible, this section will focus on the consumer protection issues across the methods of transaction which general investors are most likely to engage with such as the traditional exchange and the

[194] *Tulip Trading Ltd* v *Bitcoin Association for BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624, Paras [18-20]; *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16, Paras [26-28].

[195] For useful summaries of some of the key hacks of exchanges, see Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368. For further discussion of hacks of DEXs and other DeFi platforms see, Tom Wilson and Tom Westbrook (reuters.com), 'Hackers return $260 million to cryptocurrency platform after massive theft' (August 2021) <https://www.reuters.com/technology/defi-platform-poly-network-reports-hacking-loses-estimated-600-million-2021-08-11/> Accessed 1st February 2023.

[196] For some discussion of this potential for hacking the underlying blockchain in the context of the Ethereum unpermissioned blockchain see, Rachit Agarwal, Tanmay Thapliyal and Sandeep Shukla, 'Analyzing Malicious Activities and Detecting Adversarial Behaviour in Cryptocurrency based Permissionless Blockchains: An Ethereum Usecase' (2022) 1(2) Distributed Ledger Technologies: Research and Practice, Article 8.

DEX.[197] The exchange method and DEXs have been susceptible to hacks and scams and so could provide a significant risk for users.

One of the most prominent examples of a cryptocurrency exchange hack was the hack of Mt. Gox.[198] The mismanagement of the then industry-leading exchange resulted in Bitcoin valued at the time (2014) at nearly half a billion dollars being stolen, leading to Federal investigations, and lawsuits galore.[199] In August 2021 a DEX was hacked and had over six hundred million dollars' worth of cryptocurrency stolen.[200] Some estimates suggest that such hacks of DEX platforms in 2021 alone have totalled over ten billion dollars.[201]

For customers of the exchange or DEX, the presence of the central party (exchange or DEX) increases the ease of legal enforcement.[202] Consequently, this might raise the possibility that the customer could pursue the exchange or DEX itself, possibly under terms of the exchange's contract of service. However, liability will likely be restricted significantly in the terms and conditions of those platforms.[203] Furthermore, if a hack of an exchange or DEX results in the transfer of the cryptocurrency on the blockchain then further issues can arise. Due to the permanence of the ledger and the lack of a central party, it is likely that the cryptocurrency cannot merely be transferred

[197] The definition of immutable is "not changing, or unable to be changed" see Cambridge Dictionary, 'Immutable' (2023) <https://dictionary.cambridge.org/dictionary/english/immutable> Accessed 1st February 2023. In the context of unpermissioned blockchain technology, this means that the permanence of the network cannot be affected unless in accordance with the rules of the network. For example, the only way for transactions to be added is through validation. The term immutable is to signify that the records cannot be hacked and altered.
[198] Lawrence Trautman, 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road and Mt. Gox?' (2014) 20(4) Richmond Journal of Law and Technology 13, Part VII. For more insight into this story see, Robert McMillan (Wired.com), 'The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster' (2014) <https://www.wired.com/2014/03/bitcoin-exchange/> Accessed 1st February 2023.
[199] Ibid; Yoshifumi Takemoto and Sophie Knight (Retuers.com) <https://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228> Accessed 1st February 2023.
[200] Tom Wilson and Tom Westbrook (reuters.com), 'Hackers return $260 million to cryptocurrency platform after massive theft' (August 2021) <https://www.reuters.com/technology/defi-platform-poly-network-reports-hacking-loses-estimated-600-million-2021-08-11/> Accessed 1st February 2023.
[201] Wilson (n 38).
[202] Peder Ostbye, 'Who is Liable if a Cryptocurrency Protocol Fails?' (September 2019) <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3423681> Accessed 1st February 2023, Page 17.
[203] For an example, see binance.com, 'Terms and conditions' <https://www.binance.com/en/terms> Accessed 1st February 2023, Part IV Sections 2-3.

back to the wronged party via the peer-to-peer method. The exchanges or DEXs may be able to provide some form of compensation to affected customers but this relies on their financial capital as well as their will to compensate.[204] The following section will explore the importance of the validating nodes.

2.2.3: The honesty of the validating nodes

As discussed in section 1.3, validating nodes are the entities that validate transactions on the blockchain. In the peer-to-peer context a key risk lies with the potential for collusion by the validating nodes within a platform using unpermissioned blockchain technology. This references the infamous "51% attack".[205]

Satoshi Nakamoto, a pseudonym of the creator of Bitcoin,[206] highlights that one issue with third-party electronic payment systems is the reliance of trust placed on the intermediaries.[207] Consequently, Satoshi suggests that a centralised system renders the need for those intermediaries to act as mediators and therefore possess the capability to reverse transactions accordingly.[208] In the blockchain concept raised by Satoshi, this trust in the intermediary is theoretically replaced with cryptography.[209] As mentioned at the very outset of the whitepaper for Bitcoin, "The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes."[210] Therefore, there is a consequential degree of trust placed on the validating

[204] Yueqi Yang (Bloomberg.com), 'Crypto Exchange BitMart Vows Compensation for $150 Million Hack' (December 2021) <https://www.bloomberg.com/news/articles/2021-12-06/crypto-exchange-bitmart-to-compensate-hacked-users-ceo-tweets> Accessed 1st February 2023; Joe Tidy (bbc.co.uk), 'The real victims of mass crypto-hacks that keep happening' (August 2021) <https://www.bbc.co.uk/news/technology-58331959> Accessed 1st February 2023.
[205] Shikah Alsunaidi and Fahd Alhaidair, 'A Survey of Consensus Algorithms for Blockchain Technology' (2019) International Conference on Computer and Information Sciences (ICCIS) <https://ieeexplore.ieee.org/abstract/document/8716424> Accessed 1st February 2023, Part III.
[206] For more information on the theory of who could be Satoshi, see Banking on Bitcoin (2016) [documentary] Directed by C. Cannucciari. Netflix.
[207] Nakamoto (n 51), 1.0 Introduction.
[208] Ibid.
[209] Ibid.
[210] Ibid.

nodes, who although not operating in the mediating role, still have a degree of trust placed upon them.

In any platform that uses unpermissioned blockchain technology the incentive for an individual to mine and validate transactions must be sufficient.[211] Often in cryptocurrencies, the coins are the incentive.[212] This is a vitally important component to encourage a high enough volume of mining, which can enable the platform to run quickly.[213] In a platform using unpermissioned blockchain technology, whilst the responsibility theoretically is shared amongst peer-to-peer users, in reality, there is no obligation on any participant to maintain, update and validate for the network.

In a traditional structure, individuals would be contracted to bear this responsibility, or it may even be outsourced to companies to deal with it. The incentive for good performance in normal contractual settings is both the remuneration and the desire to not be sued for falling below the obligations. This contractual underpinning does not exist in unpermissioned blockchain technology. Therefore, the value of the incentive (the coins) plays a major role.

Validation is a timely and costly process.[214] If the value of the incentive does not outweigh the price of the output, then individuals will make no attempts to validate transactions. Without this, the platform would stagnate, and the value would rapidly decrease. The reason this is a risk for an alternative form of hacking is that it can have the potential to turn honest nodes into a majority of malicious ones. It must be noted

[211] Michael Betancourt, 'Bitcoin (Theory Beyond the Codes)' <https://journals.uvic.ca/index.php/ctheory/article/view/14792/5667> Accessed 1st February 2023, Page 1 Para 4.
[212] Melanie Swan, *Blockchain: Blueprint for a New Economy* (O'Reilly 2015), Page X.
[213] The speed of the system is seen as one of the undeniable advantages of blockchain overall (see Financial Conduct Authority (n 113), Page 11) and so ensuring this speed is key in Unpermissioned blockchain technology.
[214] Betancourt (n 211), Page 1 Paras 3-5.

that the threat of this 51% attack has not seemingly yet materialised in platforms using unpermissioned blockchain technology.[215]

However, the possibility remains. If a pool of miners did not see a significant value in mining each transaction legitimately, they may be swayed to join forces and mine with an intention of collusion. Mining is very resource intensive and aspects such as rising fuel costs could be seen to contribute to rising mining costs which can disincentivise the process.[216] The presence of mining pools will be discussed further below in Section 4.2.1 from a liability perspective.

As a result, whilst the peer-to-peer method of unpermissioned blockchain technology can be viewed as immutable, the practical operation of the technology still offers many avenues for exploitation. The common use of exchanges and DEXs within the system also provide targets for hackers to exploit. However, this is not the only area that unpermissioned blockchain technology may suffer because of. Cryptographic keys which are important in determining property ownership on the blockchain may also cause issues for immutability due to the need for the storage of the private key to be secure.[217] Hackers could seek to use malware to infiltrate individuals' storage of their private keys or individuals may forget their private key.[218] In the event of theft or loss of the private key, there is no central system or administrator that the user can recover it from.

The discussion thus far has highlighted that whilst many regard unpermissioned blockchain technology as secure, the threat of hacking remains a key risk to consider

[215] Alsunaidi and Alhaidair (n 205), Part III.
[216] For some data supporting the rising costs of mining see, (MacroMicro), 'Bitcoin average Mining costs' (January 2023) <https://en.macromicro.me/charts/29435/bitcoin-production-total-cost> Accessed 1st February 2023.
[217] Nikita Storublevtcev, 'Cryptography in Blockchain' in Sanjay Misra and others (eds) *Computational Science and Its Applications – ICCSA* (Springer Nature 2019), Page 498; Jung-Doo Koo, Seong-Hoon Oh and Dong-Chun Lee, 'Authenticated route optimization scheme for network mobility (NEMO) support in heterogeneous networks' (2010) 23 International Journal of Communication Systems 1252, Pages 1255-1256.
[218] Dhavala Lalitha Bhaskari and PSG Aruna Sri, 'A study on blockchain technology' (2018) 7 (2.7) International Journal of Engineering & Technology 418, Page 419.

both from a regulatory perspective and for users. The technology itself may be regarded as immutable[219] as there seems to be limited manifested threats occurring on the blockchain. Risks such as the potential threat of a 51% collusion, coding errors or cryptographic key theft may not provide sufficient threat currently to warrant greater regulation. It is also important to note that whilst the exchanges and DEXs may be involved in the cryptocurrency transactions they probably cannot be blamed for problems of the peer-to-peer method should they arise.

2.3: Anonymity as an obstacle to legal redress

It is clear from the previous sections that risks of coding errors or collusion exist. Individuals seeking legal redress for losses suffered because of such risks may not have a simple claim due to two key obstacles that are present. The first obstacle of anonymity of any potential defendant can be discussed here. It has been noted that anonymity is a fundamental characteristic of unpermissioned blockchain technology.[220] Whilst anonymity is present within unpermissioned blockchain technology, there is some debate as to the extent to which it is enabled. Some would argue that true anonymity is not permitted within unpermissioned blockchain technology. Rather it is a degree of pseudonymity, "using or given a false name",[221] that is permitted,[222] rather than anonymity whereby no name is given. Pseudonymity therefore can apply to unpermissioned blockchain technology as participants are somewhat identifiable via their IP addresses. However, a Virtual Private Network (VPN) can be used to hide or

[219] Zetzsche, Buckley and Arner (n 141), Page 1378.
[220] Toshendra Kumar Sharma, 'How is blockchain verifiable by public and yet anonymous?' 10th July 2018 <https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/> Accessed 1st February 2023; Balazs Bodo, Daniel Gervais and Joao Pedro Quintais, 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26 (4) International Journal of Law and Information Technology 311, Page 312.
[221] Cambridge dictionary, 'Pseudonymous' (2023) <https://dictionary.cambridge.org/dictionary/english/pseudonymous> Accessed 1st February 2023.
[222] Houben (n 60), Page 263.

mimic false locations which can obscure identities.[223] The VPN does this by technically connecting you to a false server in a different location. VPNs are commonly used for streaming activity while abroad or finding cheaper tickets for flights and are not inherently objectionable. However, with the limited identification of the real-world identity of the user already prevalent in unpermissioned blockchain technology, true anonymity is certainly practicable. As a result, there is a clear possibility of anonymity within unpermissioned blockchain technology and this can be a key obstacle for legal redress as if any potential defendant's identity is unknown, it can limit the practical application of law.

The key part to understand is the impact that such a possibility of anonymity can have on society. In this chapter, this is especially important from both the regulatory perspective and from the perspectives of the users of the technology or platforms using the technology. From a regulatory perspective, unknown identities provide a significant barrier to the enforcement of regulation.[224] Whilst legal rights could theoretically arise even when the party at fault is unknown, it would be difficult to seek legal redress if parties are anonymous in unpermissioned blockchain technology.[225] The presence of anonymity provides a significant barrier if the exchange customers try to pursue the

[223] For further discussion on this see, Paul Joan Ezra and others, 'Secured Communication Using Virtual Private Network (VPN)' in Kavita Khanna, Vania Vieira Estrela and Joel Jose Puga Coelho Rodrigues (ed), *Cyber Security and Digital Forensics: Lecture Notes on Data Engineering and Communications Technologies 71* (Springer, Singapore 2021). For an example of a company that provides a VPN service, see nordvpn.com, <https://nordvpn.com/country/britain/?gclid=Cj0KCQjwm9D0BRCMARIsAIfvfIaIC8STkwpVM1HjnQsp9a0Z_QL2rOkJNlqfMsvTbPvyyAQFGiURroQaAkg7EALw_wcB> Accessed 1st February 2023.

[224] Although in some scenarios anonymity is vital in terms of witness protection for example. Therefore, it must be treated as a balancing act. However, one can still recognise that anonymity is a threat to legal enforcement, even if it can be justified. For a brief discussion see Bjorn Lindahl (NordForsk Magazine), 'Delicate balance between anonymity and law enforcement' (February 2018) <https://www.nordforsk.org/en/news/delicate-balance-between-anonymity-and-law-enforcement> Accessed 1st February 2023.

[225] For example, in *Hamid* v *Francis Bradshaw Partnership* [2013] EWCA Civ 470, [2013] 5 WLUK 69, Lord Justice Jackson upheld the decision of the High Court by binding the 'signing party' as a party to the contract, where the contract makes no express statement that his is merely a signatory on behalf of another. In this case the court decided that a party can become the party to the contract, even when it was not his overall intention to bind himself directly. This works because the identity of the individual is known, but if that party were anonymous, it would be practically difficult to hold the online address as a party to the contract.

unknown fraudsters, as is evident in the *Fetch.ai* case.[226] In that case, fraudsters managed to gain access to Fetch.ai's cryptocurrency accounts on the exchange Binance.[227] The attackers then traded the cryptocurrency in those accounts to an anonymous buyer at a significantly undervalued price which resulted in over two and a half million dollars' worth of losses to Fetch.ai.[228] In the *Fetch.ai* case,[229] claims were made against the fraudsters and the exchange, but the key issue was that the identities and location(s) of fraudsters, as well as the location(s) of the cryptocurrencies, were unknown.[230]

The Court in this case sided with the claimants by issuing several orders to assist in the recovery of the assets.[231] A proprietary injunction in the form of a worldwide freezing order was issued against the unknown parties. Pelling J was determined to not impact innocent 3rd parties and so proprietary relief was only available against the unknown parties who "either knew, or ought reasonably to have known, [that such assets] belong to the claimant or did not belong to them."[232] A Bankers Trust Order (BTO) was also issued to obtain confidential documents from the potential defendant's bank to trace assets. Additionally, a Norwich Pharmacal Order[233] (NPO) was issued against Binance England in the pursuit of documentation and information which could

[226] *Fetch.ai Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm), [2021] WLUK 601*.
[227] Ibid, Para [3].
[228] Ibid, Para [3].
[229] *Fetch.ai Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm), [2021] WLUK 601*.
[230] Ibid, Paras [5-14]; Collyer Bristow, 'Financial Services Winter update 2021' (2nd December 2021) <https://collyerbristow.com/videos/financial-services-winter-update-2021/> Accessed 1st February 2023, Minutes 38-39.
[231] For more information see, Helen Mulcahy, 'Order, order: Fetch.AI case enhances English Courts' approach to crypto fraud' (August 2021) <https://www.fieldfisher.com/en/insights/order-order-binance-case-enhances-english-courts> Accessed 1st February 2023.
[232] *Fetch.ai Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm), [2021] WLUK 601*, Para [6]; Thomas Ash (Addleshaw Goddard), 'Fetch – The search for information by victims of cryptocurrency fraud' (Nov 2021) <https://www.addleshawgoddard.com/en/insights/insights-briefings/2021/litigation/the-brief-case-autumn-2021/fetch-the-search-for-information-by-victims-of-cryptocurrency-fraud/#:~:text=In%20Fetch%2C%20the%20Court%20granted,the%20recipients%2C%20innocent%20or%20otherwise%2C> Accessed 1st February 2023, Section 1.
[233] For discussion of Norwich Pharmacal Orders see, Kingsley Egbuonu, 'Norwich Pharmacal orders: business interests and exemplary conduct can be relevant' (2014) 9(11) Journal of Intellectual Property Law & Practice 882.

assist the tracing of assets and the identification of parties.[234] Whilst an NPO cannot be served out of jurisdiction, hence why only Binance England was served with this order, J Pelling was willing to issue the BTO outside of England which is a key legal development considering the cross-jurisdictional nature of such claims.[235]

The anonymity associated with unpermissioned blockchain technology may also be problematic for any transfer to take place with the certainty that the recipient is the intended party. This is a two-fold issue; firstly, the practical problem of ensuring the other party is whom you intend. Secondly, if an error is made, how can it be resolved? In a more traditional structure, courts could hold a centralised intermediary, for example a bank, at fault even in situations where the bank should have been on inquiry as to the transfers.[236] However, in a platform using unpermissioned blockchain technology not only is there no centralised intermediary of equivalence to a bank but the ledger is immutable. So once the property has been transferred, there is no way to return it unless the receiving party is willing to do so.

It seems relevant at this point to briefly discuss how underlying intentions of those that engage in decentralised technologies has changed. Unpermissioned blockchain technology has evolved and so should not be viewed solely as a disruptive technology.[237] Unpermissioned blockchain technology and its early uses were designed

[234] *Fetch.ai Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm), [2021] WLUK 601*, Para [48].
[235] Ibid, Para [30]; Thomas Ash (Addleshaw Goddard), 'Fetch – The search for information by victims of cryptocurrency fraud' (Nov 2021) <https://www.addleshawgoddard.com/en/insights/insights-briefings/2021/litigation/the-brief-case-autumn-2021/fetch-the-search-for-information-by-victims-of-cryptocurrency-fraud/#:~:text=In%20Fetch%2C%20the%20Court%20granted,the%20recipients%2C%20innocent%20or%20otherwise%2C> Accessed 1st February 2023, Section 2.
[236] For example, in *Singularis Holdings Ltd* (In Official Liquidation) (A Company Incorporated in the Cayman Islands) (Respondent) v *Daiwa Capital Markets Europe Ltd* (Appellant) [2019] UKSC 50, Lady Hale upheld the decision that banks have a duty of care to the customer, and where they act negligently to the detriment of the customer, they can be held accountable for it.
[237] UK Government Chief Scientific Adviser – Mark Walport (Government Office for Science), 'Distributed Ledger Technology: beyond block chain (GS/16/1) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 1st February 2023, Page 14.

in an anti-establishment manner.[238] It was formed to operate outside of regulation thus limiting the control that governments had over the technology. Whilst the original intentions of the technology may be regarded as anti-establishment, it must be said that blockchain has progressed from origins of anti-establishment cryptocurrencies which operate in contrary to more traditional systems of finance towards more revolutionary distributed systems like Ethereum.[239] Therefore, as the use of blockchain technology continues to evolve, there may be greater use of permissioned blockchains and the problem of anonymity in unpermissioned blockchain technology may become less pertinent.[240] However, for now the potential of anonymity within unpermissioned blockchain technology provides an obstacle for legal redress and must be considered in future regulatory debates.

2.4: Jurisdictional complications as an obstacle to legal redress

The second key obstacle for legal redress of the risks referenced previously arises due to the supranational nature of the technology. A decentralised ledger is capable of being accessed across the globe.[241] This can be regarded as a strength of the technology as it responds to the international character of business and can reduce costs and increase efficiency.[242] However, it can also amount to an obstacle for legal redress as it can create a degree of legal uncertainty that can only be resolved with difficulty and expense through litigation. Similar to the issue of anonymity, this is a key obstacle

[238] Amelia Schwanke, 'Bridging the digital gap: How tax fits into cryptocurrencies and blockchain development' (2017) 28 International Tax Review 20, Page 21; Erika Strebel, 'Caution is key with cryptocurrency' (2018) Wisconsin Law Journal, Page2; Phil Ariss, 'Money for Nothing?' (2017) Credit Management 13 <https://search.proquest.com/docview/1963932998?rfr_id=info%3Axri%2Fsid%3Aprimo&accountid=1469> Accessed 1st February 2023, Page 14.

[239] Robin Renwick and Rob Gleasure, 'Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems' (2021) 36(1) Journal of Information Technology 16, Page 17.

[240] For some examples of alternative uses of blockchain see Ameer Rosic (blockgeeks.com), '17 Blockchain Applications That Are Transforming Society' (2017) <https://blockgeeks.com/guides/blockchain-applications/> Accessed 1st February 2023.

[241] Tatiana Zalan, 'Born global on blockchain' (2018) 28(1) Review of International Business and Strategy 19, Page 21.

[242] Ibid.

to regulation and legal clarity, should the level of risk or harm to the public derived from interaction with unpermissioned blockchain technology become such that it warrants intervention.[243]

Hypothetically, a form of global convention would be the ideal solution to combat this problem. The uniformity that it would bring, coupled with the pooling of resources would offer the best solution for legal clarity when concerning unpermissioned blockchain technology.[244] However, a global convention requires significant collective will and consensus in the desired approach and so is not always practicably viable.[245] Due potentially to factors such as religion, culture, and politics there are wide-ranging approaches[246] and opinions on the legal approach that should be taken with cryptocurrencies, blockchain or more specifically unpermissioned blockchain technology.[247]

The difficulty of achieving consensus in international instruments creates a lack of legal clarity and whilst a global convention would theoretically provide a solution it can be difficult for nations to agree on such an approach.[248] In the absence of a convention, uncertainty as to the jurisdiction that is to settle a legal dispute can be problematic when seeking legal redress. It is important to note that conflict of laws, too, is a detailed area of law and a detailed discussion is not an aim of this chapter. As a

[243] Hari and Pasquier (n 184), Page 444.
[244] Tonya Evans, 'Role of International Rules in Blockchain-Based Cross-Border Commercial Disputes' (2019) 65 Wayne Law Review 1, Pages 7-8. For a brief discussion in the increasing consensus of global standards when regulating crypto assets see, HM Treasury (n 120), Pages 8 and 13.
[245] Willibald Posch, 'Resolving Business Disputes through Litigation or Other Alternatives: The Effects of Jurisdictional Rules and Recognition Practice' (2004) 26 Houston Journal of International Law 363, Page 364.
[246] For an example of some countries to 'ban' Bitcoin see, cryptonews.com, 'bitcoin guide' <https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm> Accessed 1st February 2023. 'Ban' is used in quite liberally, as some countries have an 'indirect ban' where trading Bitcoin is extremely difficult and inaccessible, but there is no explicit or direct ban.
[247] Savelyev (n 179), Page 559. For an interesting discussion of how there may even be internal conflicts of whether American State Law or Federal Law can apply in the context of cryptocurrency see, *In re Tezos Securities Litigation*, No. 17-CV-06779-RS (N.D.Cal. Aug. 7, 2018).
[248] For a discussion of how an international treaty can impact the application of applicable and jurisdictional law see, Christoph Schreuer, 'Jurisdiction and Applicable Law in Investment Treaty Arbitration' (2014) 1 McGill Journal of Dispute Resolution 1.

result, the discussion in this section will be based on a hypothetical situation, to highlight key jurisdictional problems and illustrate that unpermissioned blockchain technology does not fit into that system very well, and so a determination of alternative solutions may be needed.

2.4.1: Applicable law

In a traditional setting, two layers of law would need to be determined before legal redress can be granted.[249] These two layers are applicable law and jurisdictional law. The relationship between them is often important in seeking legal redress.[250] This is both from the regulatory perspective and the perspective of the individual seeking legal redress. Jurisdictional law will be discussed in the following section. Applicable law means the terms that govern the conduct.[251] These layers of law may fit more easily with contract because the parties may have agreed terms, or the law is sufficiently settled that terms can be implied.[252] As with any type of law, certain aspects can be contracted out of and other obligations, whether contractual, tortious or other, will always apply. For example, if a contractual dispute is raised in England, the courts can interpret the contract in line with English law unless a different country's law was agreed by the parties.[253] In contractual settings, the applicable law will describe the contractual terms and conditions. This commonly will be in line with the law that is to govern the contract or the *lex domicilii*. This is what the courts would need to interpret and apply.

---

[249] Ibid, Page 2.
[250] Andrew Strauss, 'Beyond National Law: The Neglected Role of the International Law of Personal Jurisdiction in Domestic Courts' (1995) 36 Harvard International Law Journal 373, Page 374.
[251] Schreuer (n 248), Page 2; Strauss (n 250), Page 376.
[252] *Modahl* v *British Athletic Federation* [2001] EWCA Civ 1447, [2002] 1 WLR 1192, Paras [35] and [100-102]. For further discussion of the test for implied contracts see, Rupert Reed QC (Wilberforce Chambers), 'Implied contract: a convenient fiction in claiming damages' (2017) <https://www.wilberforce.co.uk/wp-content/uploads/2017/01/RR-Implied-contract.docx.pdf > Accessed 1st February 2023.
[253] *Shamil Bank of Bahrain EC* v *Beximco Pharmaceutical Ltd* [2004] EWCA Civ 19, [2004] 1 WLR 1784; *Halpern* v *Halpern* [2007] EWCA Civ 291, [2008] QB 195.

In the peer-to-peer method of transaction, there exist internal rules that contain the coding protocol of the system. Yeung suggests that the internal rules effectively amount to the internal governance system and can be viewed as "code as law".[254] To enable the blockchain to remain public and decentralised and due to the anonymous nature of the blockchain, developers may struggle to introduce more specified internal rules. Salmon and Meyers highlight one example, "Generic blockchains can be put to a wide variety of uses, and there can be different data and configurations, making it very difficult for the developer to build in privacy protections adapted to the nature of the data processed on the blockchain. At best, governance rules can regulate users of the blockchain to respect privacy laws when they upload personal data to the blockchain."[255] The internal rules are unlikely to contain the intention to be legally bound and subject to formal law so the applicability of contract law is limited.[256] Courts have long recognised that words and actions of the party will be used to determine their contractual intent through an objective standard.[257] Surely where users operate via the peer-to-peer method this will be treated as indicating a *lack* of such necessary intention.

Secondly, there is the issue of whom to seek legal redress against should one of these rules be contravened. This is further complicated due to the supranational nature of the technology, whereby users can be located internationally, and many may have an ideology against involving formal law.[258] As the responsibility for maintenance and

[254] Karen Yeung, 'Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law' (2019) 82 (2) The Modern Law Review 207, Page 209.
[255] John Salmon and Gordon Myers, 'Blockchain and Associated Legal Issues for Emerging Markets' (Jan 2019) 63 International Finance Corporation 1, Page 4.
[256] Samiran Ghosh, 'Blockchain and Beyond' in Susanne Chishti, Tony Craddock and Robert Courtneidge (ed) *The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries* (Wiley 2019), Chapter 34, Page 1; Gregory Klass, 'Intent to Contract' (2009) 95 Va L Rev 1437, Page 1439; Dori Kimel, *From Promise to Contract: Towards a Liberal Theory of Contract* (Bloomsbury 2003), Pages 136-139.
[257] *Storer* v *Manchester City Council* [1974] 1 WLR 1403, Para 1408.
[258] Samiran Ghosh, 'Blockchain and Beyond' in Susanne Chishti, Tony Craddock and Robert Courtneidge (ed) *The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries* (Wiley 2019), Chapter 34, Page 1; Gregory Klass, 'Intent to Contract' (2009) 95 Va L Rev 1437, Page 1439; Dori Kimel, *From Promise to Contract: Towards a Liberal Theory of Contract* (Bloomsbury 2003), Pages 136-139. For a brief discussion on conflict of law issues see, Stephen Pitel and Nicholas Rafferty, *Conflict of Laws* (Irwin Law Inc, 2016, 2nd ed), Page 245.

upkeep in unpermissioned blockchain technology is distributed equally amongst its peer-to-peer users, in theory no single participant is at greater fault than another.[259] From a practical perspective, it would be very difficult also to pursue the whole geographically-disparate network.[260] This, combined with the issue of anonymity raised in the section prior makes the determination of applicable law problematic in unpermissioned blockchain technology.

In the absence of a contract, a person who has suffered loss through fault in an unpermissioned blockchain context may pursue a case in tort. In tort, there are overriding pre-established relationships that attract a duty of care and factors such as foreseeability, proximity and reasonableness which can also be considered to determine if a duty should exist.[261] The traditional *Caparo* test of needing to show foreseeability of harm, proximity of the relationship between claimant and defendant and whether such a claim is fair, just and reasonable to establish a duty of care[262] has been overturned in *Robinson* (2018)[263] where it is highlighted that only novel cases will fall outside of the pre-established relationships, and in those cases the law must "develop incrementally and by analogy with established authority."[264] Some pre-established relationships can include "motorists to other road users…manufacturers to consumers…employers to their employees, and…doctors to their patients"[265] to name a few. If cases are brought in tort in the context of unpermissioned blockchain technology, it will tend to be difficult to establish a duty of care based on a pre-established relationship and it is likely that this approach of incremental development will be followed.

[259] For a brief discussion of how unpermissioned blockchain technology makes no reference to any hierarchy see, Hong Kong Monetary Authority (n 66), Page 104.
[260] *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16, Paras [3-4].
[261] *Caparo Industries Plc* v *Dickman* [1990] 2 AC 605, Page 658.
[262] Ibid.
[263] *Robinson* (Appellant) v *Chief Constable of West Yorkshire Police* (Respondent) [2018] UKSC 4, Para 21.
[264] Ibid, Para 27.
[265] Ibid, Para 26.

In *Tulip Trading*,[266] the Court of Appeal recognised that a claim in tort would depend on a fiduciary relationship being established.[267] If a fiduciary relationship was held to have arisen on the facts it would require a significant development of the law on fiduciary duties. In *Tulip Trading*,[268] the defendants in the case were developers who could control who edited the software and so this does not completely align with the truly decentralised position discussed above, as there is a higher level of control exerted. However, it is still concerning unpermissioned blockchain technology as it is the Bitcoin blockchain. At this stage the Court of Appeal was determining if there was a point that should proceed to trial and were not determining that a fiduciary relationship existed.[269] The examples above signify one potential applicable law that could be applied if a legal dispute was raised in England. Tort law will be further applied to unpermissioned blockchain technology in Chapter 4.

There is an additional layer of difficulty when determining the applicable law in unpermissioned blockchain technology due to the common use of exchanges and DEXs in many cryptocurrencies that use unpermissioned blockchain technology. The exchanges and DEXs, provide a central party whose location is known and thus can help in determining relevant applicable law.[270] Some exchanges even specify the applicable law in their terms and conditions.[271] However, as stated previously, liability is often limited by exchanges and DEXs and so long as the exclusion is not unreasonable this may deny relief to users who suffer losses in the exchange or DEX methods of transaction where the fault is in the execution of the blockchain on the peer-to-peer method.

[266] *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16.
[267] Ibid, Para [41].
[268] *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16
[269] Ibid, Para [86].
[270] Ostbye (n 202), Page 17.
[271] Coinfalcon.com, 'Terms' <https://coinfalcon.com/en/terms> Accessed 1st February 2023, (Jurisdiction and Applicable Law).

As far as choice of law is concerned, English Courts have indicated that they are willing to apply English Law where the claimant was domiciled in England.[272] In the *Ion Science*[273] case, claimants brought the ex parte application for several orders to assist recovery of assets due to an initial coin offering fraud that was believed to have taken place. The potential defendants went by aliases and so were effectively anonymous. The court acknowledged the urgency of the matter and sided with the claimants by allowing them to serve via alternative means and granting the applications sought after. In the *Fetch.ai*[274] case, anonymous fraudsters accessed Fetch.ai's cryptocurrency accounts on Binance's exchange. The fraudsters then traded the cryptocurrency to an anonymous buyer at a significantly undervalued price which caused over two and a half million dollars' worth of losses to Fetch.ai. Claims were made against the fraudsters and the exchange. The Court in this case sided with the claimants by issuing several orders to assist in the recovery of the assets including international freezing orders.[275] Therefore, these cases indicate that often the *lex domicilii* of the claimant will prevail. *Lex domicilii* is defined as "the law of the domicile by which the rights of persons are sometimes governed."[276]

The *Fetch.ai*[277] case also raises a further issue when considering jurisdictional complications, namely the difficulties of enforcement. Although claims were made against the fraudsters and the exchange, the key issue in *Fetch.ai*[278] was that the identities and location(s) of fraudsters, as well as the location(s) of the cryptocurrencies,

[272] Collyer Bristow, 'Financial Services Winter update 2021' (2nd December 2021) <https://collyerbristow.com/videos/financial-services-winter-update-2021/> Accessed 1st February 2023, Minutes 43-46.
[273] *Ion Science Ltd* v *Persons Unknown and Others* (unreported) 21st December 2020 (Commercial Court).
[274] *Fetch.ai Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm), [2021] WLUK 601*.
[275] Ibid, Para [48].
[276] Merriam-Webster Online dictionary, 'lex domicilii' <https://www.merriam-webster.com/dictionary/lex%20domicilii> Accessed 1st February 2023.
[277] *Fetch.ai Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm), [2021] WLUK 601*.
[278] Ibid.

were unknown.[279] The Court in this case adopted a quick and flexible approach to side with the claimants by issuing several orders including a worldwide freezing order of assets for persons unknown who knew or ought to have known of the fraud.[280]

The *Fetch.ai* case illustrates that the exchange themselves are not the only potential defendant and there is the possibility to pursue the unknown fraudsters as courts have indicated their willingness to be flexible to protect the party that is a victim to fraud.[281] Notably, however, the effectiveness of any injunctions to freeze assets globally is heavily reliant on the cooperation of many parties both domestically and internationally, as well as the skill of investigators.[282] Even though English courts are highly respected,[283] there may be little practical benefit of an international asset freezing order if other jurisdictions do not uphold it.

For this chapter, we will continue with a presumption that the *lex domicilii* of the claimant will prevail. Although, due to the supranational nature of the technology and the potential for anonymity, the determination of applicable law is more complex than courts merely applying English law to English claimants. This section has therefore indicated the additional issues that can arise when seeking to determine the applicable law in a dispute arising through unpermissioned blockchain technology.

[279] Ibid, Para [5].
[280] For more information see, Mulcahy (n 231).
[281] Collyer Bristow (n 272), Minutes 45-47. For further discussion on this see, Albert Monichino, 'Cryptocurrency and interim court relief: Chen v Blockchain Global Ltd, CLM v CLN and Fetch.ai Ltd v Binance' (2022) 50(3) Australian Business Law Review 205.
[282] Collyer Bristow (n 272), Minutes 48-51.
[283] Dominic Raab, Ministry of Justice, 'Improving UK Competitiveness, Strengthening the Rule of Law' (Speech at the Policy Exchange, London, 7th December 2017) <https://www.gov.uk/government/speeches/improving-uk-competitiveness-strengthening-the-rule-of-law> Accessed 1st February 2023; Collyer Bristow (n 272), Minutes 49-51.

2.4.2: Jurisdictional law

Determining which legal jurisdiction can resolve disputes is a vital component of any agreement between two parties.[284] The reasons for selecting certain jurisdictions can differ. In most cases, it is a matter of convenience for one or both of the parties and often it will be where the agreement is carried out. Likewise with applicable law, where an agreement expressly states these points, things are simpler and greater clarity is offered to the parties. In the peer-to-peer method of unpermissioned blockchain technology, by contrast, legal formalities may have been purposely avoided.[285]

In theory, if a dispute was brought to the courts (discarding temporarily the issues of anonymity and other enforcement issues that have been highlighted), then cases concerning fault in unpermissioned blockchains could be brought in any country.[286] In a noncontractual case it would ultimately be the discretion of the claimant to commence litigation wherever is more favourable for their circumstances. Additionally, the supranational possibilities with unpermissioned blockchain technology makes it difficult to determine where the platform is being executed as theoretically it is distributed across the whole network of users in the variety of jurisdictions where they may be located.[287] Therefore, the user could bring the case in whichever jurisdiction is more convenient or even favourable to them.[288] An example of this can be found in *Ramona Ang* v *Reliantco Investments Ltd*[289] which involved a dispute over the client's account being terminated by the exchange and the issues pertaining to the rights of the exchange to close the account and the rights of the exchange customer to recover the

[284] Posch (n 245), Pages 363-364. It may be noted that whilst these three layers are not at the forefront of the minds of laymen, these factors are of vital importance to legal minds when determining any agreement.
[285] Yeung (n 254), Pages 212-214.
[286] Zetzsche, Buckley and Arner (n 141), Page 1392.
[287] For a discussion of this very issue but in relation to smart contracts see Hari and Pasquier (n 184), Page 444.
[288] This issue is heightened further with the use of VPN blockers as true user location/jurisdiction may also be problematic to determine.
[289] *Ramona Ang* v *Reliantco Investments Ltd* [2020] EWHC 3242 (Comm), [2020] 11 WLUK 428.

funds in the account.[290] Legal action for this dispute was raised in Germany, the Czech Republic and in England,[291] thus highlighting this potential to select a preferred jurisdiction. This means that there is no jurisdictional certainty and ultimately it is left up to the decision of the user. This highlights the difficulty of determining jurisdictional law and the need for development of approaches to handle these disruptive technologies.

The use of exchanges and DEXs can again potentially simplify the issue to some degree. If we presume that the exchange or DEX specifies in the terms & conditions that all legal disputes shall be determined by the *lex domicilii,* then the matter will be simplified to some extent. However, exchanges may specify an alternative jurisdiction that is more favourable to exchanges or may not specify one at all. Therefore, the same uncertainty of jurisdictional law may apply. It is also unlikely that the exchange could be made liable for faults in the underlying blockchain on which cryptocurrencies are operated.

As already alluded to, irrespective of jurisdictional complications, anonymity can still bring enforcement problems. This combined with the jurisdictional complications presents an unprecedented legal issue. Without the mitigation of both, there will still be significant barriers to any form of legal enforcement where there are faults in unpermissioned blockchain. As mentioned previously, these factors are difficult to resolve in a platform using unpermissioned blockchain technology, and so, if conventional means of legal redress are unavailable, potentially more unique legal approaches may be required to deal with these unique obstacles.

[290] Ibid, Para [5].
[291] Ibid.

2.5: Domestic and international political factors

The discussion of political issues in this context refers to the impact that politics can have on society and the law. One example of this could be through a potential unwillingness of governments to adopt a technology which, in the form of unpermissioned blockchain technology, prevents centralised control for the government. It is therefore more likely that governments would use permissioned blockchain technology for applications such as central bank digital currencies. However, the potential unwillingness to engage in unpermissioned blockchain technology can lead to an increase in the scepticism of society which can be an issue for unpermissioned blockchain technology itself.

> *"Governments, however, can also influence individuals' behavior in more subtle ways. They not only can pass laws that define what is or is not acceptable but can also exert indirect pressure on individuals and organizations. For example, states can use taxes to regulate markets and market participants or create new social norms over time. They can construct policies that shape the architecture of the physical or digital world from installing speed bumps near schools to slow down cars to dictating rules regarding information collection to enhance online privacy. When contemplating how to influence individuals' behavior, governments have the choice to use all or some of these different policy levers."*[292]

Therefore, by suggesting that government's use of regulation and other means can influence societal views, it could be suggested that a lack of legal clarity and a governmental unwillingness to adopt the technology could result in a degree of societal scepticism. One way to resolve this would be greater legal clarity within the field. Previously in 2.4 this thesis proposed that a global convention would hypothetically

[292] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press, 2018).

provide the best legal solution but is likely to be practicably difficult to agree and implement. Presently, tensions across the World remain unresolved. It is highly unlikely that the issue of regulating unpermissioned blockchain technology would be substantial enough to cause unity among nations.

The need for collaborative regulation especially to adapt to the technological developments in society have been noted. "Information and communication technologies (ICTs) form the backbone of today's digital economy. But creating the conditions for the new economy to flourish worldwide will require unprecedented collaboration across sectors."[293] In order to provide a greater degree of legal clarity and protection with the legal issues posed by unpermissioned blockchain technology, one suggestion could be through collaborative regulation.

Collaborative regulation in its truest form would not only require collaboration between jurisdictions but also stakeholders.[294] Collaborative regulation provides a pooling of knowledge and resources which can result in more practical and efficient forms of regulation. The formulation of some convention (whether EU based, common law based or other) would help to regulate a wider space. This could not only provide a greater degree of legal clarity for peer-to-peer users and exchange customers in these jurisdictions, but it also could solve the regulatory arbitrage issues that the New York licencing of Bitcoin exchanges faced whereby in that instance many exchanges just moved States and continued operating as they had been. By collaborating with various stakeholders, the regulation would be better informed in such a technical and novel area such as unpermissioned blockchain technology.

[293] Houlin Zhao (ITU Secretary-General), 'Collaborative regulation: Special edition, Global Symposium for Regulators (2016) 3 ITU News <https://www.itu.int/en/itunews/Documents/2016-03/2016_ITUNews03-en.pdf> Accessed 1st February 2023, Page 1.
[294] Tyler Scott, Nicola Ulibarri and Ryan Scott, 'Stakeholder involvement in collaborative regulatory processes: Using automated coding to track attendance and actions' (2020) 14 Regulation and Governance 219, Pages 219-220.

As previously noted, however, there are various legal differences that result in difficulty for uniformity of law across jurisdictions outside of a convention. Hartley refers to factors such as procedural differences, interpretational differences and differences of competence and integrity that can limit the possibility of supranational legislation.[295] One example of procedural differences can be the presence of a jury in civil trials within the US which is not the case in the UK.[296] It is clear that exploration of these political and legal differences are far beyond the scope of this thesis, however, by highlighting them one can understand that a level of global consensus necessary to lead to a convention on unpermissioned blockchain technology is unlikely.[297]

2.6: Privacy, criminal activity and the environment as additional issues

Unpermissioned blockchain technology is a novel invention that presents unique legal and societal issues in several ways. Issues such as privacy, criminal activity and the environment are examples, and each topic would be a sufficient undertaking for its own research project. Therefore, such issues will be briefly highlighted to recognise the breadth of legal issues that concern unpermissioned blockchain technology that, collectively, could present a case for greater regulation.

Data which is anonymously controlled does not necessarily fall outside of the legal remit. For example, the Data Protection Act 2018[298] specifically protects personal data and ensures that it is properly stored, and that the individual concerned has certain rights relating to that data, such as correcting inaccurate data and requesting information into the data stored.[299] The Data Protection Act recognises that some forms of data

[295] Trevor Hartley, *International commercial litigation: text, cases and materials on private international law* (Cambridge University Press, 2nd edn, 2015), Pages 7-8.
[296] Ibid, Pages 6-7.
[297] For examples of how different jurisdictions react to unpermissioned blockchain technology platforms such as Bitcoin in completely different manners, see Swan (n 212), Page 7. Additionally for a debate on how a cross-jurisdictional approach would apply to the issue of smart contracts, see Hari and Pasquier (n 184), Page 444. For a brief discussion in the increasing consensus of global standards when regulating crypto assets see, HM Treasury (n 120), Pages 8 and 13.
[298] Data Protection Act 2018 (c.12).
[299] Ibid, Provisions 2 (1) (a) and (b).

justifiably should be kept private. This can be more a question of ethics but also whether the information, if made public, could lead to some infringement on an individual's right to privacy. However, it may be difficult for data protection laws to apply where data cannot be linked back to a living individual.[300] This may render unpermissioned blockchain technology in its true peer-to-peer form, beyond the scope of the Data Protection Act 2018 as the anonymity present can limit the ease of identifying a link between the node and a living individual. Whereas, within the exchange-based method of transaction, personal information of the exchange customers is required by the exchange which creates a responsibility for exchanges to ensure that any personal information they store is secured privately and they would also have to meet other obligations within the Act itself.[301]

Another risk that is often associated with unpermissioned blockchain technology is the potential for criminal use.[302] Whilst this thesis primarily focuses on civil wrongs, it is useful for this chapter to briefly highlight the scope for criminality because it is a significant risk associated with the technology. The potential of anonymity within unpermissioned blockchain technology can mitigate the enforceability of regulation such as money laundering controls, which results in it being an attractive means for criminal financing.[303] However, for criminals to be paid for their activity, funds held as

[300] For example under EU law data protection does not apply to anonymous data under EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Article 4(1); Luca Bolognini and Camilla Bistolfi, 'Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation' (2017) 33 Computer Law & Security Review 171, Pages 176-177.

[301] Peter Chapman and Laura Douglas, 'The Virtual Currency Regulation Review – Edition 2' (2019) The Law Reviews I <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-2/1197606/united-kingdom> Accessed 1st February 2023, Section Xi.

[302] Houben (n 60), Page 261; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283, Page 284; Financial Conduct Authority (n 113), Page 12.

[303] The original intention in terms of use for criminality is unknown. What is known is the intention to not be controlled by the law, although this does not necessarily mean an intention for criminality.

cryptocurrencies may enter the regulated world through bank transfers, cash or expensive tangible assets such as diamonds, all of which have ways of being traced.[304]

One area of criminality that has been associated with the use of unpermissioned blockchain technology is ransomware and terrorist funding.[305] When hackers successfully infiltrate and take over a system of a powerful and wealthy organisation, often they will require some form of financial recompense in order to restore the control back to the original party.[306] Cryptocurrencies have now provided a useful tool for these hackers.[307] Not only can their location be hidden, but if the unique address is not tied to a particular identity then there is nothing really that agencies can do.[308] If criminals use the cryptocurrency and spend it, this can be very difficult to trace. Another example in which cryptocurrency is commonly associated with as a means of payment is the funding of terrorist activities.[309] Similarly to ransomware, the difficulty of tracing makes cryptocurrencies using unpermissioned blockchain technology very enticing for these purposes. This is a two-fold issue as it is not only difficult to determine who is receiving the funds to commit the terrorist activity, but who is funding them to do it.[310]

Another key issue, and arguably the one that is the most common forms of criminal activity that is associated with unpermissioned blockchain technology is

[304] For an explanation of how diamonds can be traced especially if stolen see, Bbc.co.uk (magazine), 'Who, What, Why: How do you spot a stolen diamond?' (February 2013) <https://www.bbc.co.uk/news/magazine-21525403> Accessed 1st February 2023.
[305] Barry Connolly (Flynn O'Driscoll), 'Cybersecurity breaches: the risks and how to mitigate them' (2017) 6(1) Compliance & Risk 7, Page 7.
[306] For an example of this, see Joe Tidy (BBC), 'How a ransomware attack cost one firm £45m' (June 2019) <https://www.bbc.co.uk/news/business-48661152> Accessed 1st February 2023.
[307] For a useful discussion on ransomware and its impact in the UK, see Mark Ward (BBC), 'Alarming rise is ransomware tracked' (June 2016) <https://www.bbc.co.uk/news/technology-36459022> Accessed 1st February 2023.
[308] Consequently, many agencies have started to focus on when cryptocurrencies are transferred into fiat currencies or other forms of currency, as this provides them the best chance to trace who may have committed the crime.
[309] Houben (n 60), Page 263.
[310] This can be an extremely complex process with various middlemen potentially involved in these types of transactions.

money laundering.[311] The capability of filtering illegal money through an anonymous cryptocurrency using unpermissioned blockchain technology presents a difficult issue for regulators and investigators. Tackling money laundering can aide the limiting of crimes as there are fewer possibilities to financially capitalise without a trace. Currently the UK has sought to mitigate the threat of money laundering through cryptocurrencies, as one of their main aims.[312] Laws were introduced to require any business conducting any crypto-asset business, to register with the Financial Conduct Authority.[313] In terms of operation, this means that exchanges would be required to register, as well as any corporation that trades in cryptocurrency, but individuals would not. This was an attempt to prevent large scale money laundering by alerting the FCA to all companies who are engaging in cryptoasset activity, the purposes in which they are doing so, and the value of such transactions.[314]

Lastly, it must be noted that unpermissioned blockchain technology has notorious environmental impacts. This is because of the computational power required in the proof-of-work form of validation method which can involve numerous computers all running continuously to compete to validate the same transaction and "mine" the same block. It has been suggested that electricity usage of Bitcoin alone could equate to the amount used by Switzerland.[315] This may be a societal concern if further use of the

[311] For an example of cryptocurrency money laundering see, Geoff White (BBC), 'UK company linked to laundered Bitcoin billions' (March 2018) <https://www.bbc.co.uk/news/technology-43291026> Accessed 1st February 2023.
[312] There is the debate of what extent national regulators can solve legal issues arising in blockchain due to its supranational nature. As suggested in this thesis, issues of anonymity and jurisdiction will not be solved but may potentially be mitigated.
[313] For an overview of these regulatory changes in the UK see Nina Moffat, Arun Srivastava and Lara Kaplan, 'New U.K. Anti-Money Laundering and Counter Terrorist Financing Requirements for Cryptoasset Businesses – Are You Ready?' (January 2020) <https://www.paulhastings.com/publications-items/details/?id=22d6886e-2334-6428-811c-ff00004cbded> Accessed 1st February 2023.
[314] Initially there was an overriding feeling that Unpermissioned blockchain technology was incapable of regulation. This shows an indication of the possibility for indirect regulation.
[315] Chris Baraniuk (bbc.co.uk), 'Bitcoin's energy consumption equals that of Switzerland' (3rd July 2019) <https://www.bbc.co.uk/news/technology-48853230> Accessed 1st February 2023. Latest figures suggest that the energy consumed for Bitcoin to run over the course of the year equates to approximately 39% of the UK's energy consumption over a year, see, HM Treasury (n 120), Page 73.

technology continues.[316] As mentioned previously, proof-of-stake provides an alternative to the proof-of-work validation method. In proof-of-stake, parties "stake" their own cryptocurrency and the protocol will automatically select the party who has staked the largest sum. Only that party will then have access to the transaction to validate it. This results in less electricity wastage and can be seen as a more environmentally friendly alternative to the proof-of-work validation method.[317]

2.7: Conclusion

The use of the technology has developed from the original peer-to-peer method to the inclusion of trades through exchanges and DEXs and may develop further.[318] The peer-to-peer method, with cryptography and other security elements, seems to be sufficiently secure and may be referred to as immutable.[319] Although, it is not without risk due to the potential threat of theft of the private key[320] and the possibility of the 51% attack.[321]

Whilst the peer-to-peer method can be regarded as effectively immutable, the same is not true of the other methods of transaction with the threat of hacking as an example being prevalent in both the exchange-based method and the DEX method.[322] These methods potentially expose users to additional risks and greater focus must be had here from an academic and regulatory standpoint. The presence of the intermediary

[316] For a discussion of Bitcoin energy consumption see, Samuel Asumadu Sarkodie, Maruf Yakubu Ahmed and Thomas Leirvik, 'Trade volume affects bitcoin energy consumption and carbon footprint' (2022) 48 Finance Research Letters, Article 102977. For some interesting figures on society's views on the environment in recent years, see Martijn Lampert (Glocalities.com), 'Global Rise in Environmental Concern' (2020) <https://glocalities.com/latest/reports/environmental-concern> Accessed 1st February 2023.
[317] For example, Ethereum's adoption of proof-of-stake as a validation method has reduced energy consumption of the platform significantly. See George Milunovich, 'Assessing the connectedness between Proof of Work and Proof of Stake/Other digital coins' (2022) 211 Economics Letters, Article 110243; Elie Kapengut and Bruce Mizrach, 'An Event Study of the Ethereum Transition to Proof-of-Stake' (October 2022) <https://arxiv.org/pdf/2210.13655.pdf> Accessed 1st February 2023.
[318] Johnstone (n 101), Page 169.
[319] Hong Kong Monetary Authority (n 12), Page 16.
[320] Bhaskari and Sri (n 218), Page 419.
[321] Alsunaidi and Alhaidair (n 205)23, Part III.
[322] Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Wilson and Westbrook (n 200).

in the exchange-based method and the DEX method may increase compatibility with traditional legal frameworks and may provide a defendant in legal claims from their customers, although further analysis into this point was beyond the scope of this chapter.[323] The methods of transaction with the technology are distinct from one another and so any legal approach must factor this in.

Furthermore, the potential for anonymity in unpermissioned blockchain technology exists and this provides the most significant obstacle from a legal standpoint.[324] The enforceability of law is threatened when the identities of parties are unknown. This coupled with the distributed responsibility of maintenance within the peer-to-peer method renders the concept of fault difficult to determine as theoretically every user within the peer-to-peer method is at fault should any risk materialise.[325] This chapter has also considered how the supranational nature of blockchain technology provides an additional obstacle for legal redress. As the likelihood of a global convention to create a uniform legal approach is limited,[326] much will depend on the approaches of the courts. Whilst English Courts have displayed a willingness to apply English Law to disputes where the claimant is domiciled in England, the effectiveness of such proceedings relies heavily on international cooperation in enforcement of judgments.[327]

Blockchain technology may have been praised for its novelty and uniqueness.[328] However, the same uniqueness can create further legal issues. Unpermissioned blockchain technology poses numerous legal issues that may be regarded as distinct

[323] Peder Ostbye, 'How Are Cryptocurrency Systems Represented and Who is Liable for Misrepresentation?' (October 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3675083> Accessed 1st February 2023, Page 17.
[324] For a brief discussion see Lindahl (n 224).
[325] Betancourt (n 211), Page 1 Para 4.
[326] Posch (n 245), Page 364.
[327] Collyer Bristow (n 272), Minutes 45-51.
[328] Balazs Bodo, Daniel Gervais and Joao Pedro Quintais, 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26 (4) International Journal of Law and Information Technology 311, Page 312.

from previous developments. Key obstacles such as anonymity and jurisdictional problems could create an impracticality for the application of traditional legal frameworks. Therefore, should legal intervention be sought by regulators, more unique legal approaches might be required to practically deal with the unique issues posed by unpermissioned blockchain technology. This will be explored throughout the thesis.

Chapter 3: Theoretical Perspectives on Liability for Systematic Faults?

3.1: Introduction and context

Chapter 2 has highlighted various risks within unpermissioned blockchain technology and some wrongs that may occur.[329] It highlighted some barriers to legal protection within unpermissioned blockchain technology.[330] The question therefore arises of who could theoretically be regarded as liable for the wrongs, providing the obstacles to redress could be mitigated? Unpermissioned blockchain technology operates as a decentralised system where the responsibility of maintenance is theoretically shared equally across the platform and so the question of liability is potentially complex.[331] A theoretical examination of liability can aid the findings of the first aspect of the research question regarding the possibility of legal redress.[332] This will build on the earlier mention of the key roles and the difficulty for a potential hierarchy of responsibility to be formed within unpermissioned blockchain technology.[333]

This chapter will also feed into the discussions of the upcoming chapters. Firstly, within Chapter 4 the application of English law in seeking to determine whether further legal redress is needed for systematic errors within unpermissioned blockchain technology, will be informed by this Chapter with respect to who should bear the liability of any proposed regulation. Furthermore, it shall influence the discussion of a self-regulatory approach to liability based on Ostrom[334] in Chapter 5 by providing some

[329] See section 2.2; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368.
[330] For a brief discussion see Lindahl (n 224); See sections 2.3, 2.4 and 2.5 respectively.
[331] Hong Kong Monetary Authority (n 66), Pages 103-104.
[332] For the discussion of the research question, see section 1.7.
[333] See section 1.3; Hong Kong Monetary Authority (n 66), Page 104.
[334] Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press 1990); Elinor Ostrom, 'Tragedy of the Commons', in Steven N Durlauf and Lawrence E Blume (ed) *The New Palgrave Dictionary of Economics* (2nd edn Palgrave Macmillan 2008).

context as to the appropriation of self-management within unpermissioned blockchain technology.[335]

For this Chapter, a determination of who could theoretically be held liable for systematic errors within unpermissioned blockchain technology shall be made. Whilst such novel technologies create some barriers to private law enforceability due to the decentralised nature and potential for anonymity, some degree of legal oversight remains important.[336] This potential for legal intervention for liability on behalf of the consumer's interests will be explored further in Chapter 4.

This chapter shall begin with a discussion of the possible rules of governance present within the peer-to-peer method of transaction under unpermissioned blockchain technology. This will inform a theoretical examination of who may be liable and whether liability can be attached to a specific role. Following this, theories that underpin liability within tort and contract will be discussed and applied to unpermissioned blockchain technology. It must be mentioned that there exist a multitude of theories within each strand of the law, and therefore it will be impractical to cover all these thoroughly. As a result, this chapter shall highlight the two most prominent theories of liability under both strands of the law mentioned above, tort and contract respectively, for the purpose of the pursuit of the research questions. Finally, there will be the discussion of strict liability and fault liability in the context of unpermissioned blockchain technology. This will involve the exploration of benefits and drawbacks within both forms of liability in the application to varying methods of transaction.

3.1.1: Internal rules

To be able to determine who theoretically may be liable for systematic errors in unpermissioned blockchains, there must be an exploration of the potential rules of

[335] See Chapter 5.
[336] Rainer Kulms, 'Blockchains: Private Law Matters' (2020) Sing JLS 63, Pages 68-69.

governance such as the internal rules in the peer-to-peer method. Yeung suggests that the internal rules and the coding of unpermissioned blockchain technology may be the only way to control the conduct of parties within the peer-to-peer method in the form of "code as law" rather than "code of law".[337] Therefore, there shall first be a discussion of the internal rules in accordance with the peer-to-peer method of unpermissioned blockchain technology.

In the traditional peer-to-peer method, it has previously been highlighted that the operation of the system is heavily dependent on the internal rules for the system and the incentives of mining.[338] Using Bitcoin as an example, there is seemingly no public information to signify the internal rules, however, there are some requirements listed to operate within the platform and fulfil the operational aspects as a "full node" within Bitcoin (also referred to as a miner).[339] These requirements often relate to the computational power and storage required in order to ensure that the network can run quickly and continuously.[340] For example, there is a requirement of a full node to have anti-virus software and other precautionary measures although there is no discussion of liability if unsuccessful.[341] Whilst the computational specifications are labelled requirements, there is the acknowledgement that you could attempt to run a "full node" (mine) even when you fail to meet all the requirements.[342] Therefore, it would be difficult to regard these requirements as having the mandatory character of rules because miners can still operate even if they fall below this standard.

---

[337] Yeung (n 254).
[338] UK Government Chief Scientific Adviser (n 237), Page 5.
[339] Miners can also be referred to as a 'full node' as they are truly operating on the platform by validating transactions. Without the role of miners, the platform would stagnate. Other roles that merely operate on the platform using unpermissioned blockchain technology and do not seek to mine or code, are not regarded as full nodes because they are not at vital for the technical operation of the platform. For a full understanding of the role of a miner see sections 1.2.4, 1.3 and 2.2.3.
[340] bitcoin.org, 'Minimum Requirements' <https://bitcoin.org/en/full-node#minimum-requirements> Accessed 1st February 2023.
[341] bitcoin.org, 'Possible Problems' <https://bitcoin.org/en/full-node#minimum-requirements> Accessed 1st February 2023.
[342] bitcoin.org (n 340).

One can assume that principles such as honesty in mining would be an underlying rule of the network as well as making every effort to ensure security by securing your wallet and the database you have. On bitcoin.org, which provides a large community-based group concerning Bitcoin, there is no direct reference to the internal rules of the system and this seems to fit more with the principle that the peer-to-peer method is not based on contractual relationships.[343] As stated previously there is also a suggestion that strict internal rules are not referenced due to the variety of data that could theoretically be stored on a blockchain and instead what is provided for is more general expectations or conventions.[344] The concept of legal risk is also mentioned but only in the sense that Bitcoin is prohibited or restricted in some jurisdictions.[345]

Instead, the broad use of internal rules which must be examined as part of the question whether code of this nature can sufficiently act as law. Within cyberspace, Lessig suggests that the code of the platform is regarded as the law of the platform.[346] If unpermissioned blockchain technology operates completely outside of the conventional legal sphere, then there may be no alternative other than treating the "code as law".[347]

Yeung proposes that there may be three categories of blockchain which may impact whether we should view code as law or acknowledge the code of law.[348] The first category is where the blockchain is intentionally designed to evade legal control, and some would argue that Bitcoin is an example.[349] The second category is the opposite extreme where the blockchain platform has been set up to be compatible with a

[343] Samiran Ghosh, 'Blockchain and Beyond' in Susanne Chishti, Tony Craddock and Robert Courtneidge (ed) *The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries* (Wiley 2019), Chapter 34, Page 1; Gregory Klass, 'Intent to Contract' (2009) 95 Va L Rev 1437, Page 1439; Dori Kimel, *From Promise to Contract: Towards a Liberal Theory of Contract* (Bloomsbury 2003), Pages 136-139.
[344] Salmon and Myers (n 255), Page 4.
[345] bitcoin.org (n 341).
[346] Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books 2006); Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999).
[347] Yeung (n 254), Page 209.
[348] Ibid.
[349] Ibid.

legal system.[350] The Maersk permissioned blockchain[351] would be an example here as the parties are identifiable and Maersk as the central party wants to conform to legal standards. The third and final category is where platforms may fall in between these two extremes.[352]

> *"The emerging response of conventional law in the first two kinds of case can be readily anticipated and understood. While the first class of case threatens to undermine the rule of law and which national legal systems can be expected to take positive action to safeguard, the second class of case does precisely the opposite: reinforcing the primacy and sovereignty of national law, and hence blockchain applications falling within this class are likely to be regarded as a welcome development by conventional legal systems. But it is the law's response to the third category of applications… that is the most difficult to predict, due to the normative ambiguity of these applications."*[353]

The difficult aspect is how to determine the scope of liability within these so called "rules of governance" combined with the concept of "code as law". If the original intentions of those who created unpermissioned blockchains were to avoid legal parameters as suggested previously in section 1.2.5,[354] then it is logical that the internal rules would not be expressly stated to limit the likelihood of contractual liability. Therefore, if these principles are more implicit and operate through code then this can justify why it is more difficult to provide a more detailed scope of liability that can then be applied to the theories throughout this chapter.[355] The vague drafting of the internal

[350] Ibid.
[351] Jesper Toft Madsen - maersk.com, 'A game changer for Global trade' Sept 2019 <https://www.maersk.com/news/articles/2019/09/20/a-game-changer-for-global-trade> Accessed 1st February 2023.
[352] Yeung (n 254), Page 209.
[353] Ibid.
[354] Hong Kong Monetary Authority (n 12), Page 34.
[355] The reliance on code will also be a concept further explored in Chapter 5 when considering the work of Ostrom and whether there is the potential of self-management in the peer-to-peer method of transaction.

rules of Bitcoin, can be interpreted as limiting potential for legal redress but not rendering it impossible.[356] The practicality of legal redress under the current framework in English law will be explored in Chapter 4 and the potential for creative legal intervention[357] will be discussed in Chapter 5. Legal theories of liability can be applied to scenarios that could arise in unpermissioned blockchain technology to determine whether there is any potential for liability to be attached to specific parties within unpermissioned blockchain technology.

3.2: Tort Theories of liability

Given the lack of contractual underpinnings for dealings on unpermissioned blockchains, tort law could provide a potential avenue for liability. Previously in this Chapter, there was the discussion of the internal rules within the peer-to-peer method.[358] This can now be applied to various theories of liability to determine whether any party may theoretically and normatively be held liable for systematic errors within unpermissioned blockchain technology.

3.2.1: Optimal Deterrence Theory

The first theory to be discussed is arguably one of the most prominent economic theories for liability.[359] It will be briefly outlined before applying it to the case of unpermissioned blockchain. As it is an economic theory at its core, it tends to focus primarily on efficiency and cost. Optimal Deterrence Theory is therefore about allocating the costs of an incident efficiently.[360] Within the law of torts you would therefore view the tort as an accident and seek to understand the cost implications for

[356] Hong Kong Monetary Authority (n 12), Pages 108-111.
[357] Ibid, Page 10.
[358] See section 3.1.1; Salmon and Myers (n 255), Page 4.
[359] Jules Coleman, Scott Hershovitz and Gabriel Mendlow, 'Theories of the Common Law of Torts' in Edward N Zalta (ed) The Stanford Encyclopedia of Philosophy, substantive revision (Winter 2015) <https://plato.stanford.edu/entries/tort-theories/> Accessed 1st February 2023, 2.
[360] James Fleming Jr, 'Optimal Deterrence and Accidents' (1975) 84(4) The Yale Law Journal 656, Page 658.

different parties involved.[361] Finding the solution to the accident involves weighing up the various cost implications on the different parties and the cost implications for any alternative or preventative measures. By viewing tort as an allocation of costs, it theoretically places the burden or cost on the party that will suffer the least.[362] Parties may logically seek insurance which provides a cost and medical bills for the injured has a specified cost, therefore, it becomes easier to determine the various costs to the parties involved.[363]

Whilst the actual theory and a deeper analysis of its application to personal injury within tort law is beyond the scope of this thesis, we can seek to apply it to unpermissioned blockchain technology.[364] Whilst the theory refers to the cost of precaution vs the cost of injury or the cost of benefit vs the cost of injury, analysis of Optimal Deterrence Theory within the context of unpermissioned blockchain technology would require the term "injury" to instead refer to the loss of value of cryptocurrency.[365]

Within the peer-to-peer method if we take the issue of outdated code for example, it seems clear that the cost to update the code would be less than the cost created through a potential collapse of the whole system.[366] A coder would be best placed to keep the code up to date. As a result, placing the liability on the coders in this scenario would be efficient theoretically as the cost for them is lower than the cost of the whole network. The cost incurred by the coder would be the financial cost of coding, which can equate "to around £20-£25 per line of new code…and about £100 per

[361] Ibid.
[362] Ibid.
[363] Coleman, Hershovitz and Mendlow (n 359), 2.
[364] For a discussion of some of the criticisms of this theory see, Fleming Jr (n 360), Pages 658-659.
[365] Hughes and others (n 171), Page 2.
[366] For some figures of collapses or hacks within the industry of cryptocurrency see Zetzsche, Buckley and Arner (n 105), Pages 1367-1369.

hundred lines of re-used code."[367] Therefore, in accordance with Optimal Deterrence Theory, the cost of precaution is less than the cost of injury or loss. This is because the cost for the coder to formulate new code would be likely to be lower than the loss that exchange-customers and the exchange could be subject to if the exchange were hacked. This then presumes that all parties are rational and so coders would actively take precaution and incur that cost in order to reduce the possibility of the loss occurring for the whole platform.[368] If the coders do not actively take said precaution knowing that the potential cost of losses to both the exchange-customers and the exchange are far greater, then it is justified that the liability will fall on the coder.

This approach could work quite simply in a more traditional organisational structure, where the coders were employed to update the code, however as mentioned previously unpermissioned blockchain technology is not a centralised structure and so operates in a unique manner. There are various issues that may arise within coding that would render the application of Optimal Deterrence Theory difficult. One issue is that code could be changed relatively regularly and so it would be difficult to determine which code, and therefore which coder may be at fault for the loss especially considering that the code may work in operation with other code or sets of code.[369] This is linked to the discussion earlier that sometimes it can be difficult to determine who is responsible for specific sets of code.[370] If there is no way of determining who is responsible for the code then the premise behind the theory falls short of any practical application.

---

[367] David Coveney (Interconnectit), 'How much does code cost?' (2008) Business <https://interconnectit.com/news/2008/06/01/how-much-does-code-cost/> Accessed 1st February 2023. Some more recent approximations suggest it could cost $100 per hour for coding/developing blockchain. For further discussion on the potential costs see, Azati.ai, 'How Much Does It Cost To Build A Blockchain in 2022' (January 2023) <https://azati.ai/how-much-does-it-cost-to-blockchain/> Accessed 1st February 2023.

[368] Robert Cooter, 'Economic Theories of Legal Liability' (1991) The Journal of Economic Perspectives 5 (3) 11, Page 15.

[369] For an example of the current coding issues that need solving see bitcoin.org, 'Fixing Existing Issues' <https://github.com/bitcoin/bitcoin/issues> Accessed 1st February 2023.

[370] See section 1.3; Zetzsche, Buckley and Arner (n 141), Page 1384.

Furthermore, as stated previously, it is difficult to determine the time that would need to pass for the current coder to have a responsibility to replace outdated code that may have been implemented by a previous coder. This then gives rise to the main underlying issue with respect to coders and more generally any of the groups highlighted previously, that there is no obligation for them to fulfil specific roles.[371] In addition to this complexity, there is room to operate within a platform using unpermissioned blockchain technology without having a specified role. As a result, it becomes more complicated to determine the scope of responsibility in which a coder for example would have in this scenario.

Now that Optimal Deterrence Theory has been applied to the peer-to-peer method, it is logical to now attempt to apply the same theory to exchanges. Leaving aside for the time being the contractual allocation of liability, the financial cost to the coder is less than the potential cost of losses to the whole network if a shutdown occurs. Within exchanges there are a few aspects that need to be addressed. Firstly, cost-efficiency will only be experienced where the issue relates to a purely exchange-based factor. An efficient allocation of costs could not be achieved where an exchange bears the responsibility for something that occurs purely within the peer-to-peer method of transacting, and this is why exclusion clauses typically apply.[372] This is because they would not necessarily be able to implement any preventative measures. As stated previously, exchanges may not even operate within the peer-to-peer method as coders or miners and so have no element of control or responsibility for issues relating to that mode. For example, any issues of security of the private key of the exchange customer or their own wallet security would be outside of the control of the exchange.[373]

[371] Swan (n 212), Page X; Betancourt (n 211), Page 1 Para 4.
[372] binance.com (n 203), Part IV Sections 2-3.
[373] For a discussion of the concept of 'wallets' and the various types that exist see, Hari and Pasquier (n 184), Pages 428-429.

In accordance with Optimal Deterrence Theory, it could be suggested that the cost of firewalls, updating coding and other security measures, would be a lower cost to the exchanges than the cost to the exchange customers and the exchange if the security was not protected, resulting in greater susceptibility to hacks and thus losses for both the exchange-customer and the exchange. The cost for the exchange is through time, money and expertise to protect the exchange and the exchange customers, whereas the potential loss to the exchange customers is the loss of value of the cryptocurrency or the theft of it altogether.

However, the significant number of exclusion clauses placed into the terms and conditions of exchanges, effectively exclude liability for the exchange of anything short of negligence.[374] Therefore although the Optimal Deterrence Theory, suggests that the most efficient place for liability to fall is the exchange itself the use of contract to exclude liability, may mean that it is rare for this protection of exchange-customers approach to tortious liability to surface practically. This limited scope of protection will be analysed in greater depth in Chapter 4 with an analysis of the exclusion clauses present covered in section 4.2.2.

As far as DEX transactions are concerned, ensuring the protection of the platform and the running of the system may be fairly attributed to the DEX under an Optimal Deterrence approach. They would bear a lower cost in investing into such protections rather than risking the platform itself being compromised. However, where they enable access to the decentralised blockchain, any errors that occur on the blockchain itself would bear a high cost of protection, and it may be practicably impossible for the DEX to control these. Alternatively, where they retain control through voting rights for the development of the blockchain then the cost of protection is likely to be lower than the risk of failure. Further discussion of relevant terms of

[374] For example, see, binance.com (n 203), Part II.

service of DEXs and who may bear the requisite risks associated will be explored in section 3.3.2. The issue here is that irrespective of the level of protection sought, the system may still be vulnerable to failing or being attacked.

3.2.2: Corrective Justice Theory

As stated previously, the Optimal Deterrence Theory is regarded as one of the most prominent economic theories applied to the law. Corrective Justice Theory would be the prime example of a popular theory not derived from economics.[375] Within this theory, there is the concept of first order and second order duties. The first order duty exists throughout time and does not arise nor cease out of circumstance. The first order duty shall prohibit conduct, for example trespass to person.[376] In a society, one can justifiably recognise why such duties shall exist, for without such legal prohibition or prevention society could dissolve into anarchy. Everyone has this first order duty and theoretically it should never be broken, however if someone does breach that first duty then a second duty shall then arise. Second order duties are duties to repair whatever has been breached because of breaking the first order.[377] Coleman suggests that…

> *"corrective or compensatory justice is concerned with the category of wrongful gains and losses. Rectification, in this view, is a matter of justice when it is necessary to protect a distribution of holdings (or entitlements) from distortions which arise from unjust enrichments and wrongful losses. The principle of corrective justice requires the annulments of both wrongful gains and losses."*[378]

Therefore, the second order duty of repair exists where loss to the injured party has occurred or gain to the other party has happened and where one or both are wrongful.

---

[375] Coleman, Hershovitz and Mendlow (n 359), 3.1.
[376] Ibid.
[377] Ibid.
[378] Jules Coleman, 'Corrective Justice and Wrongful Gain' (1982) 11 J Legal Stud 421, Page 423.

There is the presumption that where a wrongful loss has occurred to one party, the other party was wrong for not taking the precautions to avoid such a loss. This presumption can be rebutted in some rare circumstances. For example, where an individual is in a life-threatening scenario and has no alternative option but to act in a manner that may cause economic harm to another but it is necessary to save their own life then such action would still result in a wrongful loss but may be justified.[379] Nevertheless, whilst the act may have been justified, the wrongful loss incurred by the other party may still warrant the right of reparation.[380] Perry would argue that this moral dilemma of a justified action of one party that causes wrongful economic loss to another, should not influence the application of Corrective Justice Theory. "Corrective justice theorists usually fuse Aristotle's notion of corrective justice with a substantive non-consequentialist moral standard, most notably Kant's principle of right, thereby depriving corrective justice of its true meaning as a mere mathematical form."[381] Therefore, under Corrective Justice Theory where the first order duty has been breached, then the second order duty will arise to repair the damage or harm done to the other party.

In assessing peer-to-peer transactions on unpermissioned blockchains first, we can appreciate that there will still be the issues of determining who is at fault. As this has already been covered under section 1.3.1 there is no need to repeat the same points. The issues of determining which party should be accountable, in a technology that theoretically shares the responsibility of maintenance across the whole network equally, will always be an issue to consider irrespective of the theory being applied. Furthermore, applying the first order duty equally to all participants may be impractical

[379] See the scenario raised by Coleman (Coleman (n 378), Page 424) when referring to Joel Feinberg, 'Voluntary Euthanasia and the Right to Life' (1978) 7 Phil Pub Aff 93.
[380] Coleman (n 378), Page 424.
[381] Ronen Perry, 'The Role of Retributive Justice in the Common Law of Torts: A Descriptive Theory' (2006) 73 Tennessee Law Review 177, Page 178.

as for example the presence of mining pools renders the platform arguably more reliant on certain participants than others.[382] However, in a circumstance where the first order duty only arises upon fulfilling a specified role then there is the possibility that this is overcome.

As mentioned previously, the main issue would be determining who owes the second order duty of repair. Additionally, deciphering what would class as repair within the second order duty especially when considering the permanence of the network. For example, in a scenario where the miners specifically have a first order duty to "mine" fairly and justly in accordance with the rules of the network, how could a second order duty operate should the first order duty be breached? In a traditional setting, the centralised party could adjust their data and return the property to the rightful party. However, as a security measure, blockchains are immutable, which prevents any data being removed or altered once it has been validated providing that honest nodes maintain at least 51% of control.[383] Therefore, a situation could arise where malicious miners have breached their first order duty but the duty to repair is not necessarily possible. One way in which this could be solved is through a duty of repair in the value of what was stolen, with compensation being paid through a fiat currency instead of the cryptocurrency itself.

In exchange transactions the first order duties could relate to both the exchange and the exchange customers. The first order duty on behalf on the exchange would be the security of the exchange itself. For the exchange customer it would be acting in accordance with the terms and conditions of the exchange. In dealings with exchanges, it is easier to address who has breached the first order duty as the parties are known, and much like with peer-to-peer transactions, reparation may be needed in the equated value

[382] Primavera De Filippi and Benjamin Loveluck, 'The indivisible politics of Bitcoin: governance crisis of a decentralised infrastructure' (2016) 5(4) Internet Policy Review 1, Page 10.
[383] Zetzsche, Buckley and Arner (n 105), Page 1378.

of a fiat currency. Depending on the type of exchange, we may find that they do not transfer the cryptocurrency on the blockchain itself and instead just apportion their ownings of cryptocurrency amongst the exchange customers. In this scenario, if some cryptocurrency was stolen from the exchange customers, the exchange may have enough surpluses to replenish their accounts and fulfil the second order duty. However, as noted, exchange transactions will be subject to contracts that give an extremely limited scope of liability on the part of the exchange which would limit the types of first order duties that could arise or the actions that can amount to a breach in tort law. This has been covered in section 3.2.1 and so does not require greater debate here. Similar considerations would arise in relation to DEX.

Within this section, it can be stated that Corrective Justice Theory is applicable to the different methods of transaction within unpermissioned blockchain technology, although liability for exchanges is likely to be excluded under contract. The resolution to these proposed issues of determining who is at fault in peer to peer and DEX transactions will impact on whether the law can sufficiently operate within this sphere.

As the main theories of liability that can be applied to tort have been covered so far and applied to unpermissioned blockchain technology, it seems logical to now proceed with the theories of liability that can be applied to contract law and then apply those theories to unpermissioned blockchain technology likewise.[384]

3.3: Contractual Theories of liability

Various theories shall be discussed in this section building upon the previous mapping of responsibilities and liabilities that have been discussed in section 3.2. Some issues such as allocating responsibility for faults in peer-to-peer transactions and the exclusion of liability in exchange transactions have already been covered therefore,

[384] It is worth noting that for the purpose of this thesis there was no significant differences between Corrective Justice Theory and Distributive Justice Theory, hence the latter not being covered here. For further discussion on this see Coleman, Hershovitz and Mendlow (n 359), 3.1.3.

shall only be touched upon where relevant. It is important to re-emphasise that formal contract law does not seem compatible with the peer-to-peer method and so the focus on contractual theories may have greater application with the exchange-based method and possibly the DEX.

3.3.1: Promise Theory

Epstein refers to Fried[385] in the notion of Promise Theory.

> *"If I make a promise to you, I should do as I promise; and if I fail to keep my promise, it is fair that I should be made to hand over the equivalent of the promised performance. In contract doctrine this proposition appears as the expectation measure of damages for breach."*[386]

This theory fundamentally goes to the root of the principle of a formation of a contract. It dates back to a principle whereby your word is a powerful promise or bond and should therefore, be a respected covenant between yourself and another to whom you have given your word.[387] One of the key aspects of contract and indeed in a liberal view of one's life is the freedom to choose and act in a manner one desires, providing it does not result in the exploitation of others.[388] Liability should justifiably be attached to an individual who freely makes a promise and consequently breaks that same promise without good reason.

In applying this theory to the peer-to-peer transactions based on unpermissioned blockchain technology, it provides an interesting analysis. The first question to ask would be what aspect of the unpermissioned blockchain technology can amount to a promise of this nature? The answer would seemingly be the internal governance rules of

[385] Charles Fried, *Contract as Promise: A Theory of Contractual Obligation* (Oxford University Press 2015, 2nd edn).
[386] Richard Epstein, 'Beyond foreseeability: consequential damages in the law of contract' in Raymond Gillespie Frey and Christopher Morris (eds) *Liability and responsibility: essays in law and morals* (Cambridge University Press 1991), Pages 91-92.
[387] This notion of an individual's word being their bond is echoed in Fried (n 385), Pages 64 and 73.
[388] Ibid, Page 7.

the platform using unpermissioned blockchain technology. If, from a theoretical standpoint, everyone that participates within the platform using unpermissioned blockchain technology provides that promise to each other, then theoretically anyone could be liable, although the one pursued is likely to be the one with the deepest pockets. However, as stated previously, there are differing roles within unpermissioned blockchain technology and so this can develop the analysis further.[389]

One could state that there are general promises given for the whole network, but when an individual takes up a specified role within the platform using unpermissioned blockchain technology, then more specified promises are attached to that party. For example, in *Tulip Trading*,[390] there was the discussion regarding the specific roles of developers and miners in the underlying blockchain and whether either role may have sufficient power or control to rectify an error in the underlying blockchain.[391] However, the issue with this concept of general promises is that Promise Theory seemingly only applies to express terms of the contract and does not account for any implied terms. Whilst in practise within contract law, promises or terms may be implied, Promise Theory focuses primarily on the justification for liability of breaches of an explicit promise.

One example of the specified role having specific promises could be where an individual takes up a role such as a miner; they may be implicitly making a promise to mine honestly. If they were to mine dishonestly, then they should be liable for this as they would be breaking their promise in accordance with the Promise Theory. In the *Tulip Trading* case,[392] the defendant's argue that the principle of decentralisation creates

[389] See section 1.3; Hong Kong Monetary Authority (n 66), Page 104.
[390] *Tulip Trading Ltd* v *Bitcoin Association for BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624; *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16.
[391] *Tulip Trading Ltd* v *Bitcoin Association for BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624, Paras [32-35]; *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16, Paras [32-34].
[392] *Tulip Trading Ltd* v *Bitcoin Association for BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624; *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16.

a sense of interdependency amongst users although there was some dispute in the case as to the level of control that miners have.[393] If for example Promise Theory was applied to a different role, such as a coder, would the promise made by the coder be to code to the best of their abilities? Alternatively, the promise could potentially be to code within the common practises of coding at the time. Whilst the same issues can arise with respect to determining who or which specific code is at fault there is also the issue of specifying what promises would be made where they are not specified within the internal rules and where they are inferred.[394] It appears that if promises of this nature are not referenced within the internal rules,[395] then Promise Theory would not operate to include implied promises.

By contrast an exchange's promise may be defined in their terms and conditions or more generally it could be regarded as a general promise of security of the exchange which would incorporate not only the security of the cryptocurrency, but the personal information of customers held by the exchange. Whilst the explicit terms and conditions of the exchange will govern the conduct and promises made, there is scope also for more general implied terms to be included. There could be standard implied terms, as in sale of goods law, where there is an implied term that goods are of satisfactory quality.[396] A similar principle of implied terms could be developed in the context of exchanges for a general promise of security of the exchange as stated above which could not be excluded by contract.

DEXs are likely to follow that of the exchange whereby terms and conditions provide a structure for promises to be made between the DEX and DEX customer.

---

[393] *Tulip Trading Ltd* v *Bitcoin Association for BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624, Para [34]; *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16, Para [33].
[394] For the discussion surrounding determining which code or coder is at fault see section 3.2.
[395] For more debate on the concept of the internal rules, see section 3.1.1; Salmon and Myers (n 255), Page 4.
[396] Section 14 Sale of Goods Act 1979; Section 9 Consumer Rights Act 2015.

Further discussion of DEXs terms and conditions will be provided in the following section. The scope for implied terms would therefore also provide a potential. Although where a DEX is truly decentralised the difficulty of specifying what promises are made will be akin to the peer-to-peer method. In applying Promise Theory to unpermissioned blockchain technology it could potentially create more flexibility in the scope of the promises made or implied promises made, which could enable a common law system to seek a balance between protection and over-burdening.

Therefore, Promise Theory could provide useful standards that individuals would have to conform to in unpermissioned blockchain dealings as well as in trades on exchanges and DEX. However, if Promise Theory is taken strictly to apply only to express terms or express promises then it would not be beneficial as a theory of liability for peer-to-peer transactions. In a common law system such as England, standards or implied promises could potentially develop accordingly within the common law. Lord Wilberforce in the *Panalpina* case[397] states that there is a progression of contract law "away from the rigid theory of autonomy towards the… imposition – by the courts of just solutions".[398] This can suggest that where implied terms may provide a more just outcome, the courts may be willing to utilise the flexibility afforded to them in the interpretation of contract through the common law, although there are likely to be difficulties in developing such an approach in the blockchain context. It can be somewhat difficult to determine what promises may be given in dealings with unpermissioned blockchains unless they are specified in the internal rules. In trades through exchanges (and potentially DEXs) the promises are likely clearer due to the existence of an express contract but likely to limited within the terms and conditions.

[397] *National Carriers Ltd* v *Panalpina (Northern) Ltd* [1981] AC 675.
[398] Ibid, Page 696; Andrew Morris, 'Practical reasoning and contract as promise: Extending contract-based criteria to decide excuse cases' (1997) 56(1) Cambridge Law Journal 147, Page 153.

3.3.2: Consent Theory

Consent Theory is another significant theory with respect to contractual liability.[399] Consent Theory is essentially the notion that where one consents to a contract, this consent is to all the terms of that contract both expressly stated and implied.[400] Consent Theory can therefore be distinguished from Promise Theory as it accounts for the implied rules to a contract, the objective terms applied rather than the purely subjectively expressed terms.[401] There is a suggestion that practically Promise Theory and Consent Theory must be viewed in tandem with one another.[402] This is because they account for the express terms and the implied terms separately but in reality contract law grants validity to both and so Promise Theory and Consent Theory must be combined in order to adequately account for liability within contract law.[403]

By applying Consent Theory to different types of dealings with unpermissioned blockchain one must acknowledge a freedom to contract in any matter the individual sees fit, provided it is not illegal.[404] Therefore, one should first look at the internal governance rules which every participant has at least impliedly consented to through operating in this unique platform. One issue could arise as to the concept of "consent" for a purely contractual purpose. It must be stated at this point that this is not a discussion of the definition of "consent" overall, but purely in a contractual setting.[405]

---

[399] James Maxeiner, 'When Are Agreements Enforceable? Giving Consideration to Professor Barnett's Consent Theory of Contract' (2006) 12 IUS Gentium 92, Page 93.
[400] Randy E Barnett, 'Rights and remedies in a consent theory of contract' in Raymond Gillespie Frey and Christopher Morris (eds) *Liability and responsibility: essays in law and morals* (Cambridge University Press 1991) Pages 140-141; Maxeiner (n 399), Page 98.
[401] Randy E Barnett, 'Rights and remedies in a consent theory of contract' in Raymond Gillespie Frey and Christopher Morris (eds) *Liability and responsibility: essays in law and morals* (Cambridge University Press 1991) Page 148.
[402] Epstein (n 386); Barnett (n 401), Page 148.
[403] Further to this, a combination of both theories with Entitlement Theory, arguably provides the most accurate description of contractual liability. This view would allow for the freedom of contract (consent) to be noted within an agreement of an exchange of rights (promise), which is confined by what rights the law recognises (entitlement). Entitlement Theory is more easily applied in the context of public law and did not require further analysis here. For further discussion see, Epstein (n 386) Page 95; Barnett (n 401) Pages 136-137 and 148.
[404] Barnett (n 401) Page 141.
[405] For discussion of informed consent in the context of blockchain see, Zhen Zheng, *The Legal System of Art Auction in China* (Springer 2022), Pages 143-149.

The question therefore arises in involvement with unpermissioned blockchains where individuals have two realistic choices: either consent to the expectations or conventions which fall short of strict rules and operate within the platform or do not use the platform. The issue here is whether true consent can be achieved when there is no alternative available for operation within the platform. The only way to use the platform is to consent completely to those rules. However, in operating within the peer-to-peer method do all peer-to-peer users consent (impliedly) to a lack of legal redress? As the internal rules of Bitcoin for example do not explicitly state any aspects of legal redress, Consent Theory could only feasibly apply to the peer-to-peer method to account for the possibility of implied terms.

The potential approach to unpermissioned blockchain can be likened to the *specificity of sport* and the World Anti-Doping Agency (WADA) rules which govern professional sport. When applying the Law to sport one must take "into account the specific nature of sport, its structures based on voluntary activity and its social and educational function".[406] Athletes have two effective choices, much like those who involve themselves with unpermissioned blockchains: either conform to the WADA rules, or do not become a professional athlete. Another similarity arises between WADA and peer-to-peer methods of unpermissioned blockchain technology, often the justification for enabling WADA to set these strict confines is the protection of sport and the *specificity of sport* or "spirit of sport" itself.[407] One could make the argument that the internal rules are for the protection of the platform itself and that the law may apply a degree of "specificity of blockchain" to the way the law operates within this field. This will be another factor considered in Chapter 4.

[406] Article 165 Treaty on the Functioning of the European Union (TFEU).
[407] World Anti-Doping Code (2015 with 2019 amendments) <https://www.wada-ama.org/sites/default/files/resources/files/wada_anti-doping_code_2019_english_final_revised_v1_linked.pdf> Accessed 1st February 2023, Page 14.

Contract Law could potentially apply with greater simplicity to the peer-to-peer method of unpermissioned blockchain technology if the vague internal rules are supplemented by implied terms to increase the opportunity for legal redress for peer-to-peer users within unpermissioned blockchain technology. The final issue is whether any form of contract would be practical in the context of unpermissioned blockchain technology due to the shared responsibility and anonymity that is present. These are factors as stated previously, that would have to be considered to better understand whether legal redress for systematic errors within unpermissioned blockchain technology is practical under the current English legal approach.[408]

Turning to exchanges, their customers could be said to consent to the volatility of the market and therefore consent to the risk of losing money because of the fluctuations in value.[409] Exchange customers could also be regarded as consenting to additional risks providing that the exchanges do what they can to ensure security of the network in accordance with their terms and conditions. These additional risks could include hacks of the exchange unless the exchange acts in a manner almost amounting to negligence as highlighted earlier.[410]

Regarding the DEX transactions, the DEX customers may consent to the lack of intention to be legally bound on the decentralised blockchain. Therefore, potentially in doing so, they would only seek liability against the DEX company in the context of their relationship as DEX and DEX customer but could not pursue the DEX for faults that occur on the blockchain. It is also relevant to note that DEXs may also utilise exclusion clauses to limit the scope of their liability. For example, the top three DEXs in

[408] For more discussion see Chapter 4.
[409] For an example of the terms and conditions stating specifically the volatility within cryptocurrencies see, Coinfalcon.com (n 271), (Risk Warning); Tap.global, 'Terms and conditions' <https://www.tap.global/cryptocurrency-terms-and-conditions> Accessed 1st February 2023, Clause 2 (Risk Warnings).
[410] For example, see, binance.com (n 203), Part II.

respects of market share according to CoinMarketCap,[411] dYdX, Uniswap (V3) and Kine Protocol contain several clauses in their terms of use stating that the user must be aware of the risks present and will hold the DEX harmless from any claim derived from using their services.[412] Consequently, the DEX will mirror the peer-to-peer and exchange-based methods depending on context.

Therefore, it appears that Consent Theory could fill in some of the gaps highlighted with Promise Theory in the previous section, by implying some terms into the agreements in the three methods of transaction. This would solve the issue of whether the express terms are all that can qualify as a party's bonds or whether additional terms could be implied or set as a standard. Consent Theory, combined with Promise Theory could provide an underlying concept for the development of a framework for liability within this field.[413] It is also relevant to note that these implied standards of promises that could apply, could develop sufficiently under the common law in a manner akin to the *specificity of sport*, albeit the "specificity of blockchain" potentially.

3.4: Strict or fault-based liability?

As discussed previously, there is a fine balance between trying to enable sufficient protection via the law and over-burdening those whom it affects.[414] Analysing whether strict liability or fault liability would be more suitable for unpermissioned blockchain technology is merely another facet that must be considered to ensure that

[411] (coinmarketcap.com), 'Top Cryptocurrency Decentralized Exchanges' (February 2023) <https://coinmarketcap.com/rankings/exchanges/dex/> Accessed 1st February 2023.
[412] (dydx.com), 'Terms of Use' (February 2023) <https://dydx.exchange/terms?> Accessed 1st February 2023, Paras 10-11; (uniswap.org), 'Uniswap Labs Terms of Service' (November 2022) <https://uniswap.org/terms-of-service> Accessed 1st February 2023, Assumption of Risk-Indemnity; (docs.kine.im), 'Terms of Use' (February 2021) <https://docs.kine.im/library/terms-of-use> Accessed 1st February 2023, (1)-(3).
[413] Entitlement theory was also explored in line with these theories; however, it more closely deals with public law, therefore, detailed discussion was not necessary. For more discussion of Entitlement Theory and its potential applicability to contract law see, Epstein (n 386) Page 95; Barnett (n 401) Pages 135-139; Michael Davis, 'Necessity and Nozick's Theory of Entitlement' (1977) 5(2) Political Theory 219, Page 220.
[414] Cooter (n 368), Page 12.

this careful balance of fairness and protection is achieved. To understand this further, definitions of both strict liability and fault liability are needed.

Strict liability can be defined as "Liability… that is imposed without the necessity of proving [intention]…[or] fault."[415] Traffic offences such as speeding or parking on a double yellow line are strict liability offences but this approach is a special aspect for the law and is not representative of the approach to the law concerning other aspects within society.[416] If strict liability were imposed, a key issue would be the fairness across the different methods of transaction. In the peer-to-peer method, strict liability on coders for coding errors would likely deter coders from developing the network which may stifle innovation and could further embed weaker platforms into the market.[417] Additionally, it would not resolve the issue of identifying potentially anonymous parties. As stated previously, there is no benefit in the formulation of law that provides only theoretical rights and no practical rights.[418] In the exchange-based method, the key issue would be whether strict liability may overburden the exchange themselves. Although potentially it could be utilised from the perspective of ensuring regular security checks of the exchange are carried out. Similarly, the issue of potentially overburdening might be present regarding DEX platforms. For example, if the DEX company is held strictly liable for issues that occur on the blockchain itself, this would be unfair where the blockchain is truly decentralised from them and they do not retain any control.[419]

[415] Jonathan Law and Elizabeth Martin, *A Dictionary of Law* (Oxford University Press 2009, 7th edn), 'Strict liability'.
[416] For an interesting discussion of how strict liability could benefit a specific area of the law see, Harry Newman and David Wright, 'Strict Liability in a Principal-Agent Model' (1990) 10 International Review of Law and Economics 219.
[417] For further discussion on the threats of such a paternalistic approach see, Stacey Dogan and Mark Lemley, 'Antitrust Law and Regulatory Gaming' (2009) 87 Texas Law Review 685. For a discussion of how strict liability is designed as a deterrent technique see, Cooter (n 368), Pages 11-12.
[418] Zetzsche, Buckley and Arner (n 105), Page 1405; See section 2.3.
[419] For more discussion of the potential lack of decentralisation in a DEX see, Kruppa (n 93).

Fault liability is defined as "a type of liability in which the plaintiff must prove that the defendant's conduct was either negligent or intentional; fault-based liability is the opposite of strict liability."[420] It has been suggested that whilst strict liability operates as a presumption of fault, fault liability requires the proof that such a fault exists.[421] Whilst one could argue that contract law follows a strict liability approach,[422] fault liability is more commonly associated with contractual liability.[423] Applying fault liability to the peer-to-peer method would not be appropriate as the peer-to-peer does not have a formal law underpinning it. In the exchange-based method, exchanges may contract out of some liability through their terms and conditions of service. In the context of DEXs, fault may be difficult to prove depending on the extent that the DEX is decentralised and would depend on whether the error occurs on the blockchain or whether the DEX company has provided the error.

As a result, it appears that there are issues with both strict liability and fault liability in its application to unpermissioned blockchain technology. This should form no surprise as liability within unpermissioned blockchain technology does not currently offer legal clarity and is the legal issue at the core of this thesis.[424] Additionally, this discussion further indicates that unpermissioned blockchain technology may require creative regulation such as the potential use of strict liability in specified circumstances to provide some degree of protection to the end users.[425]

---

[420] Kermit Hall, *The Oxford Companion to American Law* (Oxford University Press 2002), 'Fault Liability'.
[421] George Cohen, 'The fault that lies within our Contract Law' (2008) 107 Michigan Law Review 1445, Page 1445.
[422] Robert Scott, 'In (Partial) Defense of Strict Liability in Contract' (2008) 107 Michigan Law Review 1381, Page 1381.
[423] For example, the principle of force majeure clauses in contract are that where an event occurs whereby no party is at fault then the parties will be relieved of their obligations under the contract. See, Barry Nicholas, 'Force Majeure and Frustration' (1979) 27 American Journal of Comparative Law 231, Page 237. For some interesting discussion on the significance of force majeure clauses in a wider scope than natural disasters, see Jennifer Smith and Andrew Behrman, 'The importance of a strong force majeure clause in an unstable geopolitical environment' (2015) 8(2) Journal of World Energy Law and Business 116.
[424] See sections 1.4 and 1.6 for a discussion of why this issue is important.
[425] Zetzsche, Buckley and Arner (n 105), Page 1405; Financial Conduct Authority (n 113), Pages 13-14.

3.5: Conclusion

This chapter has provided insight into the rules of governance within unpermissioned blockchain technology and who theoretically could be held liable within each of the methods of transaction. In relation to unpermissioned blockchains, the internal rules do not provide the assistance that could be expected.[426] The internal rules of the blockchains, with the Bitcoin blockchain as the prime example, relate mostly to eligibility to be involved in the operation.[427] The lack of legal terminology or hints to legal frameworks would appear to conform with the initial development of unpermissioned blockchain technology and its original anti-establishment nature.[428] As the technology develops, there is scope for some platforms to transition slightly away from this and so we may see internal rules in the future which can be more closely associated with a legal framework. However, presently they do not provide the basis for legal liability.

In contrast, exchanges tend to adopt clear legal terminology and an intention to form contractual relations through the terms and conditions of service of the exchange. This conforms to the expectations of contractual liability and some terms and conditions can clearly reference jurisdictional and applicable law to govern any disputes.[429] However, many clauses within the terms and conditions are exclusion clauses, limiting the liability of exchanges to the point where it appears that negligence may even be required if the exchange is to be pursued for fault.[430] Some exchanges specify alternative dispute resolutions as the avenue rather than court proceedings.[431] The effect of the contractual limitations of exchanges is minimal legal protection for exchange customers. Depending on the nature of the formulation of the DEX, it may be more akin

[426] Salmon and Myers (n 255), Page 4; See section 3.1.
[427] bitcoin.org (n 340); See section 3.1.
[428] Hong Kong Monetary Authority (n 12), Pages 108-111; See section 3.1.
[429] Coinfalcon.com (n 271), (Jurisdiction and Applicable Law).
[430] binance.com (n 203), Part II.
[431] Coinfalcon.com (n 271), (Using CoinFalcon's Services, S7).

to the peer-to-peer method whereby there is a lack of clarity for legal liability, or it may operate as more of a traditional exchange where terms and conditions limit liability. From the discussion of some of the terms and conditions of DEXs, it appears that the latter is a strong possibility where some level of control is retained by the organisation that oversees the DEX.

Furthermore, this chapter sought to apply various theories of liability to further inform the possibility of legal redress for systematic errors within unpermissioned blockchain technology. By providing some examples and scenarios of systematic errors and applying the theories to them, a fuller picture of potential liability could be made, although there will be challenges in enforcement of claims, as discussed in Chapter 2. As for exchanges, liability is often restricted through exclusion clauses which mitigates the potential for legal redress and no further protection is likely to be present in the DEX method of transaction either. Strict liability was also considered as a possibility but is one which would not seem immediately to be needed in the context of unpermissioned blockchain technology due to the presently limited degree of public harm.

Chapter 4: Doctrinal Analysis of the Extent to which English Law Currently Might Provide Redress for Loss Caused by Systematic Errors within Unpermissioned Blockchain Technology

4.1: Introduction

Having considered liability in contract and tort from a theoretical perspective this chapter offers a discussion of whether users within an unpermissioned blockchain technology system can reasonably expect that the traditional legal framework will adequately deal with the risk of errors. If there exist sufficient protections currently, then it lessens the case for regulation. Alternatively, any indications that the current legal framework does not provide sufficient protection, may suggest a reason to further explore the possibility of regulation. This chapter will therefore inform Chapter 5 as to whether a risk of a lack of redress presents a case for regulation, either by itself or in combination with other risks.

This chapter firstly considers the formation of a potential claim in contract and tort law respectively, as the most likely grounds for redress. There is no detailed discussion of claims in equity, given the likely difficulties of establishing fiduciary relationships within the decentralised system, in the absence of special circumstances. In the High Court in *Tulip Trading*[432] for example, it was determined that no fiduciary duty arose on the facts,[433] although, the Court of Appeal,[434] stated that there was an issue to be tried on this matter.[435] Nevertheless, the Court of Appeal in *Tulip Trading*,[436] did recognise that it would be unlikely for a fiduciary duty to be found in a truly decentralised system, but would be possible if the governance was not truly

[432] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624.
[433] Ibid, Para [97].
[434] *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16.
[435] Ibid, Para [91].
[436] *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16.

decentralised.[437] The fact that it remains a triable issue provides the possibility that the common law may develop in this area and this is supported as the judge signifies "If the decentralised governance of bitcoin really is a myth, then in my judgment there is much to be said for the submission that bitcoin developers, while acting as developers, owe fiduciary duties to the true owners of that property."[438] Thus, if the platform using unpermissioned blockchain technology does not operate in a truly decentralised manner, some roles within the system could have fiduciary duties attached to them should case law develop accordingly. It remains important to note that in a truly decentralised system, attaching liability to specific roles in a uniform manner has already been discussed in section 1.3.1 and would be problematic. Therefore, it could be stated that the imposition of fiduciary duties in a truly decentralised system "would be impractical",[439] due to the lack of a hierarchy of roles within the unpermissioned blockchain technology platforms.[440] As roles in unpermissioned blockchain technology, such as mining, are highly incentivised but not obligatory, it can be difficult to attach a standard of a duty of care (if any) that a particular role must uphold.[441] This can be further complicated due to the cross-jurisdictional nature of unpermissioned blockchain technology.[442] Therefore, the application of fiduciary duties seems to be incompatible with a decentralised system.

The second aspect that requires focus, is whether the potential claims in contract and the tort of negligence are practicably enforceable and there will be an evaluation of the current level of protection afforded to peer-to-peer users, exchange customers and

[437] Ibid, Para [91].
[438] Ibid.
[439] Raina Haque and others, 'Blockchain Development and Fiduciary Duty' (2019) 2 Stanford Journal of Blockchain Law and Policy 139, Page 186.
[440] See section 1.2.1.
[441] For a discussion of the incentivisation present in unpermissioned blockchain technology see, Ajay Kumar Shrestha, Julita Vassileva and Ralph Deters, 'A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives' (2020) Frontiers in Blockchain <https://www.frontiersin.org/articles/10.3389/fbloc.2020.497985/full> Accessed 1st February 2023.
[442] Walch (n 81), Page 76.

DEX customers for losses arising from systematic errors. Various problems may arise when seeking to apply these traditional frameworks to a novel technological structure like unpermissioned blockchain technology, such as seeking to identify a potential defendant when the technology enables a degree of anonymity.

4.2: The Formation of Legal claims

4.2.1: The peer-to-peer network

As blockchain is a developing technology, there is a degree of uncertainty that remains concerning how the law may apply. This section will explore the potential for contractual and tortious claims to be brought resulting from an error on the peer-to-peer method of transacting.[443] Within unpermissioned blockchain technology, one complicating factor in establishing a contract is the potential for anonymity.[444] There has already been the discussion of whether true anonymity exists in unpermissioned blockchain technology,[445] but for this thesis, it was determined that two parties may interact with each other on the blockchain without knowing who the other party is or having any identifiable factors of the other party.[446] It can therefore be more difficult to determine who are the parties to a particular claim within unpermissioned blockchain technology in comparison to a traditional business relationship.

[443] Although it must be noted that there is also the discussion of how smart contracts will fall into the traditional contractual law framework, this is not the focus of this thesis. For more discussion on the Law Commission's view that the common law is flexible enough to include smart contracts in its parameters see, Law Commission, *Smart Legal Contracts Advice to Government* (Law Com No 401, 2021) Paras 4.91-4.92. For further discussion on whether contract law can currently deal with smart contracts and how it may be incorporated see, Matja Djurovic and Andre Janssen, 'The Formation of Blockchain-based Smart Contracts in the Light of Contract Law' (2018) 26(6) European Review of Private Law 753. For more discussion on smart contracts see, Andreas Bogner, Mathieu Chanson and Arne Meeuw, 'A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain' IoT'16: Proceedings of the 6th International Conference on the Internet of Things (November 2016) 177 <https://doi.org/10.1145/2991561.2998465> Accessed 1st February 2023.

[444] Houben (n 60), Page 263.

[445] See section 2.2.

[446] Marco Conoscenti, Antonio Vetro and Juan Carlos De Martin, 'Blockchain for the Internet of Things: A systematic literature review' (2016) IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7945805> Accessed 1st February 2023, Page 2.

In traditional business settings, many organisations "would take much greater care when contracting with relatively unknown parties".[447] Such parties are not anonymous or unidentifiable but lack a pre-established working relationship and so are treated more cautiously. For example, in international trade, documentary credits[448] and bills of lading are of vital importance for trust to be established between parties often through an intermediary.[449] However, such caution is not present in unpermissioned blockchain technology as the trust is placed in the technology rather than the individual party. In a traditional business setting, a contract can provide a safety net as the parties' rights and obligations are specified often in the contract and will hold those parties to their contractual obligations. Whereas in unpermissioned blockchain technology, if the parties are unknown, then the users may ultimately lack the safety net of contractual law.

This anonymity creates a significant problem for the formation of a legal claim, irrespective of whether the party who suffers loss seeks remedies in contract or tort law.[450] The obligations or duties in contract or negligence rely on the ability to know the parties involved and also their actions/omissions to determine liability.[451] This becomes problematic when the real identity of the participant is unknown, as is the case in unpermissioned blockchain transactions. Anonymity does not present an

[447] Hugh Beale and Tony Dugdale, 'Contracts between Businessmen: Planning and the Use of Contractual Remedies' (1975) 2 Brit JL & Soc'y 45, Page 47.
[448] "A documentary credit is the written promise of a bank, undertaken on behalf of a buyer, to pay a seller the amount specified in the credit provided the seller complies with the terms and conditions set forth in the credit." See Edward Hinkelman, *A short course in International payments: how to use letters of credit, D/P and D/A terms, prepayment, credit, and cyberpayments in international transactions*, (2nd edn World Trade Press 2009), Chapter 10, Page 50.
[449] Dr Mohd Hwaidi and Graham Ferris, 'Switching from Paper to Electronic Bills of Lading: Fundamental Sociological Structure, Distributed Ledger Technology and Legal Difficulties (2019) 24(4) Journal of International Maritime Law 297, Pages 300 and 310.
[450] Collyer Bristow (n 272), Minutes 32-34; Peder Ostbye, 'Exploring The Role of Law in The Governance of Cryptocurrency Systems and Why Limited Liability DAOs might be a Bad Idea' (January 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007547> Accessed 1st February 2023, Page 17.
[451] Nick Sage, 'Contractual Liability and the Theory of Contract Law' (2019) 30(3) King's Law Journal 459, Page 473; For an interesting discussion of how contractual liability may be regarded as an automatic liability, see Nick Sage, 'Contractual Liability and the Theory of Contract Law' (2019) 30(3) King's Law Journal 459, Pages 473-475.

unsurmountable obstacle under civil and criminal procedure rules, judges do have a wide range of tools available that can mitigate the problems of anonymity as well as specialist investigators who can track down anonymous parties. These rules can assist victims and, for example, proceedings can begin in an expedited manner, without notifying the potential defendants.[452]

In unpermissioned blockchain technology, there is no written agreement or other formal contract and the parties themselves may benefit from the anonymity where there is "the impossibility to link an address of the blockchain system with a real identity or an IP address, and also the impossibility to understand that different addresses of the system belong to the same user."[453] Therefore, even if the particular participant that is at fault could be pinpointed in the system, their real identity may be difficult to determine.

There are "internal rules" of governance within the unpermissioned blockchain technology platforms, for example in the Bitcoin system based on "governance by the infrastructure (achieved via the Bitcoin protocol) and governance of the infrastructure (managed by the community of developers and other stakeholders)."[454] The former is achieved through the underlying processes of the code. It may however be difficult to establish any form of implied contractual agreement in this context as it provides the coding infrastructure for the system to function but does not create relevant duties of parties. The coding infrastructure may appear to be more promising in terms of determining a contractual agreement. Key changes to the system rely on the principle of consensus being achieved. Therefore, the parties that accept such a change are theoretically agreeing to the change and there is the possibility to analyse whether this could provide the basis of a contractual agreement.

[452] Collyer Bristow (n 272), Minutes 32-35.
[453] Conoscenti, Vetro and De Martin (n 446), Page 2.
[454] De Filippi and Loveluck (n 382), Page 1.

Two main issues can arise when determining whether a contract could be formed here. Firstly, parties may be regarded as consenting to the risk of errors that may arise from accepting the change even where they are not accepting potential liability for such harm. The second point is more important in that, for a contract to be formed the parties must intend to be contractually bound.[455] Factors such as the language used and the location of the contractual negotiations are important for the determination of such intent to form contractual relations.[456] Intent is viewed as a vital component upon which the formation of a contract may be determined.[457] This provides a major issue when assessing the concept of unpermissioned blockchain technology due to this technology's anti-establishment origins and the underlying desire to operate outside of legal parameters.[458] Those involved in unpermissioned blockchain technology, often have no desire to create legal relations as the belief is that parties can rely on the immutability of the technology and do not require legal interference.[459] Indeed, "One of the primary drivers behind the success of blockchain is an anti-establishment set of beliefs."[460] It is important to note that whilst this anti-establishment origin was present in the Bitcoin blockchain, those presently transacting with Bitcoin do not necessarily have the same motives. It has previously been recognised that "Blockchain technologies have since evolved from anti-establishment digital currencies operating outside mainstream financial systems to a 'revolutionary' technological blueprint for distributed computing

[455] *Hadley* v *Kemp* [1999] 4 WLUK 377, Page 623.
[456] *Blue* v *Ashley* [2017] EWHC 1928 (Comm), [2017] 7 WLUK 593, Para [56]; *Chitty on Contracts* (32nd edn, 2015) Vol 1, Paras 2-177, 2-194 and 2-195.
[457] Gregory Klass, 'Intent to Contract' (2009) 95 Va L Rev 1437, Page 1439; Dori Kimel, *From Promise to Contract: Towards a Liberal Theory of Contract* (Bloomsbury 2003), Pages 136-139.
[458] Stephen Wilson and David Chou, 'How Healthy is Blockchain Technology' (2017) Proc HIMSS AsiaPac17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3668102> Accessed 1st February 2023, Page 1.
[459] Adam Sanitt (Norton Rose Full Bright), 'Smart Contracts' (November 2019) <https://www.nortonrosefulbright.com/en/knowledge/publications/1bcdc200/smart-contracts> Accessed 1st February 2023, Introduction section.
[460] Samiran Ghosh, 'Blockchain and Beyond' in Susanne Chishti, Tony Craddock and Robert Courtneidge (ed) *The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries* (Wiley 2019), Chapter 34, Page 1.

architectures, such as Ethereum."[461] A traditional legal framework may therefore become more compatible with unpermissioned blockchain technology, depending on the underlying coding of the blockchain and the attitudes of the users.

To the extent that blockchain technology is an anti-establishment attempt to strip powers away from governmental control, it may be regarded as a success. "Regulators are operating under the assumption they may join the development at a later stage when necessary restrictions have been identified… such a strategy may not be possible, as protocols that are coded into the system currently may be impossible to remove or replace later on, especially given the decentralised nature of system governance, and the lack of any identifiable controlling entity."[462] The very nature of the technology, which lacks a centralised governance system, and the presence of anonymity essentially mean that the law will only be compatible when the blockchain wants it to be. A blockchain such as the Bitcoin blockchain which is inherently anti-establishment showcases no desire to create formal legal relations and so it is unlikely a court will ever determine that there is such an intention, expressly or impliedly.

Courts have long recognised that words and actions of the party will be used to determine their contractual intent through an objective standard.[463] Surely the actions of operating via the peer-to-peer network, rather than transacting through the intermediary of an exchange, will be treated as indicating a lack of such necessary intention. However, one issue that may arise in such circumstances is that in applying this objective standard, courts must adopt the position of a "reasonable person" in the position the party was in.[464] LJ Steyn in the *First Energy*[465] case stated that one of the underlying principles of contract law is that if there is a reasonable expectation from an

[461] Renwick and Gleasure (n 239), Page 17.
[462] Ibid, Page 30.
[463] *Storer* v *Manchester City Council* [1974] 1 WLR 1403, Para 1408.
[464] *First Energy (UK) Ltd* v *Hungarian International Bank Ltd* [1993] 2 Lloyd's Rep 194.
[465] Ibid.

honest person that a contract would be formed, then contract should protect this.[466] One issue that may arise here, is whether a "reasonable man" would wish to operate outside of legal control. However, it must be noted that this is not the question that is likely to be asked. The purpose of applying the objective standard is to determine whether a "reasonable man" in that same scenario is likely to have had the intention to form a contract. Within the peer-to-peer system of the Bitcoin blockchain, for example, the answer is likely to be no.

It is unlikely that the courts would find a contract to be present where there is a lack of legal intention to be contractually bound. Contract law does involve some presumptions. For example, there is a presumption that household or social agreements do not have the intention to create legal relations.[467] Alternatively, there is a presumption of such intention when concerning commercial transactions, unless there is clear evidence to the contrary.[468] Due to the lack of express contract in unpermissioned blockchain technology, and the perceived underlying lack of intention to be legally bound, it is highly unlikely that courts will seek to determine the formation of a contract in such circumstances. Therefore, it appears that in the traditional peer-to-peer system, the formation of a contract can largely depend on the underpinnings of the blockchain itself. Consequently, peer-to-peer users within the Bitcoin blockchain for example would not be likely to be able to seek legal redress through contract law in England even if they suffered harm because of a systematic error.

At first glance, the tort of negligence may offer better prospects for redress for faults in unpermissioned blockchain technology as it caters to the concept of cumulative liability well.[469] This can be important in a decentralised platform whereby the

[466] Ibid, Page 1410.
[467] *Balfour* v *Balfour* [1919] 2 KB 571.
[468] *Esso Petroleum Co* v *Customs and Excise Commissioners* [1976] 1 WLR 1.
[469] See *Fitzgerald* v *Lane* [1987] QB 781 as an example where two negligent defendants and the claimant were all deemed responsible.

responsibility or liability cannot just fall on a central party. "Unpermissioned distributed ledger systems like Bitcoin lack a central legal entity with formal responsibility over the system."[470] Instead, the responsibility of maintenance of the network is theoretically shared equally amongst peer-to-peer users. In theory, each participant can operate in several different roles including mining. In practice, mining is often done in "pools" of dedicated mining resources. "Since it is difficult for an individual miner to find a block, miners usually join one or more mining pools and contribute their computing power to the pools."[471] Some calculations of blocks mined on the Bitcoin blockchain suggest that almost 70% of the mined blocks have been done by "mining pools".[472] Almost half of those have been fulfilled by five mining pools alone.[473] Other suggestions claim that currently 75% of the network is controlled by "mining pools", most of which are based in China.[474] This may suggest that greater liability could be attached to these mining pools as they may be deemed to control a greater proportion of the blockchain.

Within the peer-to-peer model, it is likely to be very difficult to apportion fault to differing roles. Due to the decentralised structure of the platform, no individual party or role is obliged to fulfil that role. Instead, their operation is highly incentivised. "The Bitcoin ledger is constructed in a distributed and 'permissionless' fashion, so that anyone can add a block of transactions if they solve a new cryptographic puzzle to add each new block. The incentive for doing this is that there is currently a reward in the form of… [6.5] Bitcoins awarded to the solver of the puzzle for each 'block'."[475] If the

[470] UK Government Chief Scientific Adviser (n 237), Page 45.
[471] Rui Qin, Yong Yuan and Fei-Yue Wang, 'Research on the Selection Strategies of Blockchain Mining Pools' (2018) 5(3) IEEE Transactions on Computational Social Systems 748, Page 748.
[472] BTC.com, 'Pool Distribution' (January 2023) <https://btc.com/stats/pool?pool_mode=all> Accessed 1st February 2023.
[473] F2 Pool – 9.86%, AntPool – 8.99%, BTC.com – 5.10%, Braiins Pool – 5.06% SlushPool – 5.0% and BTC Guild – 4.26%, see Ibid.
[474] De Filippi and Loveluck (n 382), Page 10.
[475] UK Government Chief Scientific Adviser (n 237), Page 5. The figure of 6.5 has been updated according to, Hossein Jahanshahloo, Felix Irresberger and Andrew Urquhart, 'Bitcoin Under the Microscope' (November 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4273839> Accessed 1st February 2023, Page 6.

value of Bitcoin decreases, less incentive is provided to the miners or mining pools and this could threaten the operation of the blockchain. Over time, with the decrease in the value of the reward, the incentive could decrease also depending on the value of Bitcoin. From a liability perspective, this creates a problem as each role within the system is not structured traditionally, such as through contracts of employment. As a result, roles of miners and coders for example are not set and constantly rely on the financial incentivisation and the incentivisation of the running of the system.

The decentralised, incentivised nature of roles[476] within unpermissioned blockchain technology renders it difficult to determine any form of governance structure[477] or hierarchy and therefore it can be difficult to attach fault to a particular role such as coders for example. The main issue therefore in bringing a claim of negligence for an error within the peer-to-peer model is determining which party should bear the fault when theoretically the responsibility is shared equally. Even in a circumstance where a party can be deemed responsible for the error that occurs, such a party may be anonymous which would render a legal claim impractical.[478] Additionally, as noted in the *Tulip Trading* case,[479] traditionally liability has not been imposed for omissions or failing to act where there is no positive duty to protect[480] or in accordance to *Smith* v *Littlewoods*[481] where it is somewhat foreseeable that the 3rd party may cause damage.[482] This is present in the context of coding errors as failure to update code can be regarded as an omission which is generally not recoverable unless there was a

[476] For a discussion of the incentivisation present in unpermissioned blockchain technology see, Shrestha, Vassileva and Deters (n 441).
[477] Hong Kong Monetary Authority (n 66), Page 104.
[478] Paulo Tasca and Riccardo Piselli, *The Blockchain Paradox* (Oxford University Press, 2019), Chapter 1, Page 31.
[479] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624.
[480] Ibid, Paras [87-88]; *Smith* v *Littlewoods* [1987] AC 241, Pages 271C and 278C.
[481] *Smith* v *Littlewoods* [1987] AC 241.
[482] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624, Para [89].

positive duty to update it. Furthermore, parties should not be held liable for losses incurred by 3rd parties.

Furthermore, the second key problem that could arise is that the financial loss suffered because of systematic errors within a cryptocurrency blockchain may not be recoverable in tort. Whether or not damages should be recoverable for pure economic loss is a highly contentious area for debate and is a topic beyond the scope of this chapter.[483] Pure economic loss may be regarded as harm suffered because of negligence that causes no physical damage and is solely financial.[484]

The first point to note is that in the context of faulty coding, the pure economic loss would be derived from that of a negligent act/omission rather than a negligent statement. The relevant law is therefore *Spartan Steel*[485] where the court confirms this concept that property damage is recoverable in tort, but pure economic loss is not. It is relevant to note that in case such as *AA,*[486] *Ion Science*[487] and *Wang,*[488] cryptocurrency constitutes property under English Law. Although these cases concern issues of fraud and recovery of assets, the characterisation of cryptocurrency as property creates an interesting prospect within tort law as losses concerning cryptocurrency could be viewed as property damage rather than pure economic loss. Although this may enhance the potential for legal claims, courts may not approach it in such a manner and there would also be the issue of whether a duty of care is owed. In *Tulip Trading,*[489] this point was raised, and they stated that the losses suffered was purely economic as there was no

[483] John G Fleming, *The Law of Torts* (9th edn, North Ryda, NSW: LBC Information Services 1998), Page 194.
[484] Christian Witting, 'Duty of Care: An Analytical Approach' (2005) 25(1) Oxford Journal of Legal Studies 33, Page 45.
[485] *Spartan Steel & Alloys Ltd* v *Martin & Co (Contractors) Ltd* [1973] QB 27.
[486] *AA* v *Persons Unknown & Others* [2019] EWHC 3556 (Comm), [2020] 4 WLR 35.
[487] *Ion Science Ltd* v *Persons Unknown and Others* (unreported) 21st December 2020 (Commercial Court).
[488] *Wang* v *Darby* [2021] EWHC 3054 (Comm), [2022] Bus LR 121.
[489] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624.

"physical harm to person or property."[490] Furthermore, the court stated that it would be important to take an incremental approach here and this suggests it will be unlikely for this categorisation to alter soon in respect of tort law.[491]

If cryptocurrency loss is viewed as pure economic loss, the general rule is that this is not recoverable within the tort of negligence.[492] In the *Customs & Excise*[493] case, it was stated that such a duty would be assumed between parties if the nature of the relationship would seemingly satisfy a contract except for consideration.[494] As noted in *Tulip Trading,*[495] the key aspect here is whether there is a special relationship amounting to a fiduciary duty and whether there is a voluntary assumption of responsibility.[496] As mentioned in section 4.1, in *Tulip Trading,*[497] it was held that no fiduciary duty arose on the facts[498] and this is likely to be true in a peer-to-peer manner of transacting. Although in the Court of Appeal,[499] whilst discussing whether there was an issue to be tried on the basis of a fiduciary duty, the court determined that this was an issue to be tried.[500] The court did acknowledge that for the case of fiduciary duty to be made successfully there would need to be a substantial change in the common law[501] but "if the decentralised governance of Bitcoin really is a myth, then in my judgment there is much to be said for the submission that bitcoin developers, while acting as

[490] Ibid, Para [86].
[491] Ibid, Paras [86], [102] and [160]. The Court of Appeal's discussion (*Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16) of whether there was a triable issue as to the existence of a fiduciary duty did not discuss the concept of pure economic loss in tort, but it remains to be seen whether further guidance will be provided as this case progresses.
[492] Ryan Lee and Nickolaus Ng, 'A Tale of Two Common Law Systems: Robinson and Spandeck – Comparing the Test for Duties of Care in Singapore and England (2022) Singapore Comparative Law Review 134, Page 143; *Spartan Steel & Alloys Ltd* v *Martin & Co (Contractors) Ltd* [1973] QB 27.
[493] *Customs & Excise Commissioners* v *Barclays Bank plc* [2006] UKHL 28, [2007] 1 AC 181.
[494] Ibid, para [4].
[495] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624.
[496] Ibid, Paras [91-92] and [97-99].
[497] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624.
[498] Ibid, Para [97].
[499] *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16.
[500] Ibid, Para [91].
[501] Ibid, Para [86].

developers, owe fiduciary duties to the true owners of that property."[502] Therefore, it is possible that case law may develop to find the presence of a fiduciary relationship although the present common law approach would suggest this is unlikely.

Whether a fiduciary relationship is found, the issue of whether a duty of care exists may still warrant discussion. However, it is recognised that even in the application of the *Caparo*[503] test which is a standard used to determine whether a party owes a duty of care, judges have some flexibility of application.[504] The first point to consider under the *Caparo* test is whether harm is foreseeable.[505] Harm is likely foreseeable in a circumstance where a coder negligently coded for a platform for example. This would render it vulnerable to attacks and it is foreseeable that personal data may be stolen, or financial loss may incur. The second part of the test involves an assessment of the proximity between the potential defendant and claimant. [506] Proximity may be more difficult to determine due to the shared responsibility of maintenance and the length of time that may have passed since the code was embedded. It would be difficult to then show that one particular coder could be proximate to a potential claimant when considering the decentralised and potentially anonymous nature of operating on the platform. The final principle under *Caparo* for establishing a duty of care is whether such an imposition would be fair, just and reasonable. [507] It would be unlikely for courts to determine that any faults arising from coding would be fair, just and reasonable to then hold the coder liable in such circumstances due to the decentralised nature of the platform. This may extend the scope of liability too far and

[502] Ibid, Para [91].
[503] *Caparo Industries PLC* v *Dickman* [1990] 2 AC 605.
[504] Marilena Stylianou, 'Pure Economic Loss in Negligence: Has England Got It Wrong – Does Australia Have It Right' (2011) 1 Southampton Student Law Review 20, Page 31.
[505] *Caparo Industries Plc* v *Dickman* [1990] 2 AC 605, Page 658.
[506] Ibid.
[507] Ibid.

place too great a burden on any party that fulfils the coding responsibility of the platform. Therefore, it does not seem likely that a duty of care would be established.

The key point to highlight is that there remains the judicial freedom to provide an assessment of whether the harm suffered should warrant the imposition of a duty of care. Such freedom provides for issues of policy to be considered and may create a degree of uncertainty in its application.[508] There remains a cautiousness to open the floodgates of claims for pure economic loss,[509] and such cautiousness is likely to remain in the context of claims within unpermissioned blockchain technology. Given the likely difficulties in gaining redress, this raises the issue of the policy choice of regulators and whether they feel that the risk is severe enough to intervene. This will be discussed in more depth in the following chapter.

4.2.2: Liability of exchanges

As has been referenced throughout the thesis, the divergence of the network which includes both peer-to-peer transactions and those through exchanges is vitally important to any legal analysis. The two models are fundamentally distinctive from one another and so must be analysed separately. The presence of the exchange increases the potential applicability of the traditional legal framework including contract and tort law. However, their existence does not increase the chances of redress for coding errors on the underlying blockchain as an example because exchanges are normally removed from this process. Exchanges "are easier targets for enforcement, and may also be suitable targets for class action suits."[510] So far the regulatory response in the UK has been to focus on public harm as the FCA has sought to require a registration system for exchanges to mitigate the potential for money laundering within the realm of

[508] Ryan Lee and Nickolaus Ng, 'A Tale of Two Common Law Systems: Robinson and Spandeck – Comparing the Test for Duties of Care in Singapore and England (2022) Singapore Comparative Law Review 134, Page 144.
[509] Ibid, Page 143.
[510] Ostbye (n 202), Page 17.

cryptocurrency,[511] although the latest consultation about cryptoasset by the UK government opens the possibility for further regulation in the future.[512] Such an approach could suggest that exchanges may also provide a potential defendant to be pursued by the exchange customer in the event of losses arising from systematic errors.[513]

In 3.1.1 the internal rules of unpermissioned blockchains were discussed and there was the determination that they are more akin to conventions or expectations than strict rules. This was important from a theoretical perspective for the understanding of how the peer-to-peer method may be incompatible with theories of liability. As this section will explore the practicality of contractual claims in the exchange-based method of transaction, it is important to explore the terms and conditions of the exchanges to further inform the discussion.

Crypto exchanges typically follow a traditional contractual framework.[514] Since the main focus of this thesis is unpermissioned blockchains, a thorough investigation of all cryptocurrency exchanges in the UK is beyond the scope of this thesis. Instead, three exchanges were analysed to better understand the types of terms and conditions present in cryptocurrency exchanges. These exchanges (Binance, OKEx and Coinbase Pro) were selected as they are the top three "centralised exchanges" (meaning they are controlled by a specified party) based on their global rankings on the Coingecko site in terms of a normalised trading volume per 24 hours.[515]

[511] Financial Conduct Authority, 'Cryptoassets' (2019) <https://www.fca.org.uk/consumers/cryptoassets> Accessed 1st February 2023.
[512] HM Treasury (n 120), Pages 10-11.
[513] Ostbye (n 202), Page 18.
[514] See the reference to contractual terms in terms and conditions of exchanges. For example, BitGem, 'terms and conditions' <https://www.thediamondloupe.com/sites/awdcnewswall/files/attachments/pinkcoin-sales-terms_0.pdf> Accessed 1st February 2023.
[515] This is in accordance with the information on coingecko.com as of the 13th of September 2020 See, coingecko.com, 'Top Cryptocurrency Exchanges Ranking by Trust Score – Spot' <https://www.coingecko.com/en/exchanges> Accessed 1st February 2023.

Various clauses in the exchanges' terms and conditions indicate a clear intention to create contractual obligations. For example, some terms and conditions require users to accept that disputes shall be resolved through the means of arbitration.[516] Due to flexibility of negotiations and sometimes cheaper costs of arbitration, it may be a viable form of alternative dispute resolution in comparison to formalised court proceedings.[517] Other dispute resolution options may provide alternative benefits such as the speed of proceedings. The form of ADR that is most suitable in any given circumstance is highly fact dependent. Additionally, unique forms of resolution which operate in specific industries and function based on fixed fees such as Online Dispute Resolution (ODR),[518] domain names dispute resolution (UDPR policy)[519] or documents-only dispute resolution (e.g., DOCDEX)[520] may signify the potential for the formation of an alternative dispute resolution to be catered specifically for unpermissioned blockchain technology, or cryptocurrencies or exchange-based cryptocurrencies for example.

As alluded to in Chapter 2, determining applicable and jurisdictional law is very important when seeking legal redress.[521] Often in the peer-to-peer method of transaction, the relevant applicable and jurisdictional law is left unspecified; however,

---

[516] okex.com, 'Terms of service' <https://www.okex.com/support/hc/en-us/articles/360021813691-Terms-of-Service> Accessed 1st February 2023, S20; Koray Caliskan, 'The Elephant in the Dark: A New Framework for Cryptocurrency Taxation and Exchange Platform Regulation in the US' (2022) 15(3) Journal of Risk and Financial Management 118, Page 124.

[517] Paul Bennet Marrow, Mansi Karol and Steven Kuyan, 'Artificial Intelligence and Arbitration: The Computer as an Arbitrator – Are We There Yet?' (2020) 74(4) Dispute Resolution Journal 35, Page 70. For a brief summary of some benefits of arbitration as a form of Alternative Dispute Resolution see, citizensadvice.org, 'Using Alternative Dispute Resolution to solve your consumer problem' <https://www.citizensadvice.org.uk/scotland/law-and-courts/legal-system-s/settling-out-of-court/using-alternative-dispute-resolution-to-solve-your-consumer-problem-s/> Accessed 1st February 2023.

[518] For an interesting discussion on the legitimacy of ODR see, Dr Mohammed Khair Mahmmoud Al-Adwan, 'The legitimacy of Online Alternative Dispute Resolution (ODR)' (2011) 2(19) International Journal of Business and Social Science 167.

[519] For more information see, ICANN.org, 'Uniform Domain-Name Dispute-Resolution' <https://www.icann.org/resources/pages/help/dndr/udrp-en> Accessed 1st February 2023; Tony Willoughby, 'Domain name disputes: the UDPR 10 years on' (2009) 4(10) Journal of Intellectual Property Law & Practice 714.

[520] For greater understanding of DOCDEX see, iccwbo.org, 'DOCDEX' <https://iccwbo.org/dispute-resolution-services/docdex/> Accessed 1st February 2023; Andrii Zharikov, 'Resolving Disputes Without Reference to National Laws: analysis of the nature and practice of Documentary Instruments Dispute Resolution Expertise (DOCDEX)' (2022) 33(10) International Company and Commercial Law Review 507.

[521] Hari and Pasquier (n 184), Page 444.

the terms of exchanges can expressly reference and limited the law governing contracts to a specific jurisdiction. For example, "This agreement will be governed and the exclusive jurisdiction of the English courts."[522] Limiting the jurisdiction brings greater certainty in a complex area.

It is very common to find as part of general terms and conditions a number of clauses which seek to limit the liability of one contracting party.[523] A reduction in the potential liability of the exchange will increase their protection from being pursued for fault or errors within the system.[524] All three of the exchanges analysed regard the terms and conditions as a legally binding contract between the exchange and the exchange customer,[525] but seek to indemnify themselves from any issue not referenced within their terms and conditions and seek to limit liability for anything referenced.[526] The issue therefore is not whether liability is limited but whether there remains an adequate form of redress for the exchange customers of exchanges.

From an analysis of the exchanges mentioned above, exclusion clauses are commonplace. The three exchanges that were thoroughly analysed all included extensive liability exclusion clauses within their terms and conditions, typically providing that the exchange shall not be liable for any errors that the exchange itself is not directly responsible for. In circumstances where the exchange is expected to take responsibility, the terms provide that the exchange shall be absolved of any liability providing that the exchange acted reasonably. These clauses effectively limit the liability of the exchange only to factors they directly control and set a threshold of a

[522] okex.com, 'Terms of service' <https://www.okex.com/support/hc/en-us/articles/360021813691-Terms-of-Service> Accessed 1st February 2023, S13.19.
[523] The justification for the selection of which exchanges have been analysed will be made in due course.
[524] For an example, Binance state that to the maximum extent of the law they remove liabilities whether express or implied, so far as the law provides binance.com (n 203), Part IV Section 1.
[525] For an example, coinbase specifically state that it is a contract see, coinbase.com, 'coinbase user agreement' <https://www.okex.com/support/hc/en-us/articles/360021813691-Terms-of-Service> Accessed 1st February 2023.
[526] binance.com (n 203), Part IV Sections 2-3.

reasonable standard. This means they will not bear liability for faults that occur directly on the blockchain and will only be liable for faults in the exchange that occur in the event of negligence.

Binance for example limits its liability to cases where the fault is as "a result of Binance's gross negligence, fraud, wilful misconduct or intentional violation of law. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation may not apply to you." This approach can be compared to the liability of agents in a contractual setting.[527] Providing the agent acts within their scope of agency and is therefore merely an agent of the principal, no liability can be attached the agent itself. With exchanges, providing they do not act outside of their scope as an exchange, then liability would seemingly not fall upon them. One example where an exchange was successfully pursued by the customer for the actions of the exchange occurred in *Ramona Ang* v *Reliantco Investments Ltd,*[528] where the High Court determined that Reliantco's closure of Ms Ang's account, closing of open positions held and denial of her withdrawing the funds amounted to a breach of contract under the terms and conditions of the user agreement.[529] The court determined that Reliantco did not have the right to close the account under the circumstances at hand and even if they did, there were various protections that should be afforded to Ms Ang under the Consumer Rights Act 2015, that clauses in the contract to annul or cancel the account on such a basis were deemed unfair under Section 62.[530] This case

[527] Edward Mearns, 'Vicarious liability for agency contracts' (1962) 48(1) Virginia Law Review 50, Page 51. For further discussion of the principal agent relationship in the UK see, Jane Broadbent, Michael Dietrich and Richard Laughlin, 'The Development of Principal-Agent, Contracting and Accountability Relationships in the Public Sector: Conceptual and Cultural Problems' (1996) 7(3) Critical Perspectives on Accounting 259.
[528] *Ramona Ang* v *Reliantco Investments Ltd* [2020] EWHC 3242 (Comm), [2020] 11 WLUK 428.
[529] Ibid, Paras [83-87] and Para [107].
[530] Consumer Rights Act 2015 c15; *Ramona Ang* v *Reliantco Investments Ltd* [2020] EWHC 3242 (Comm), [2020] 11 WLUK 428, Para [89]. There was also the consideration of whether English Law or Cyprus Law governed the agreement, but the court determined that their decision would remain the same under both, see, *Ramona Ang* v *Reliantco Investments Ltd* [2020] EWHC 3242 (Comm), [2020] 11 WLUK 428, Para [90].

highlights the possibility of an exchange customer pursuing the exchange, but only for matters which result in a breach of the terms and conditions or for action taken by the exchange under a provision which is unfair under consumer protection law. Therefore, providing the exchange acts in accordance with their terms and conditions and do not act negligently, then no liability will befall them.

Some exchanges allocate risk to the customer. Naturally "The user shall bear any loss [resulting from] his/her own fault or error."[531] Additionally, there is a mention in some terms and conditions of the various risks in cryptocurrency.[532] The "risk" noted on OKEx is regarded as significant, and it is expressed that the exchange customers bear the risk for the volatility within the market.[533] This principle is similar to that of caveat emptor in contract.[534] There must be some responsibility placed on the individual who chooses to invest in cryptoassets which are inherently risky as it could place far too great of a burden on the seller if they had to bear full responsibility. Although, if this is compared with the extensive regulatory framework for the London Stock Exchange, as an example whereby there are stringent requirements for the shares listed, it may suggest that regulators could impose such a responsibility on the exchange itself.[535] It is important to note here that such an obligation would create stringent requirements for listing cryptocurrencies on the exchange but it ought not to lead to the exchange being liable for all losses incurred in investment. Even if the claimant has a valid claim, it will be worthless if the defendant is insolvent, similarly to victims of Ponzi schemes whereby upon seeking to claim liability, the victim will not be able to benefit of any

[531] For an example of such a clause see, okex.com (n 522), S3.
[532] For example, see, binance.com (n 203), Part III.
[533] coinbase.com (n 525), S3.
[534] Henry Campbell Black, *Black's Law Dictionary* (2nd edn Lawbook Exchange 1995), Page 422.
[535] Section 73A Financial Services and Markets Act 2000 grants the FCA right to alter and update such listing rules which can be found here, Financial Conduct Authority, 'The Listing Rules' (January 2023) <https://www.handbook.fca.org.uk/handbook/LR.pdf> Accessed 1st February 2023.

additional protection where the wrongdoer's funds have been exhausted.[536] This conforms to the current legal approach in England which primarily focuses on warning users of the risks present within the market and that there is minimal legal protection afforded to the end users in the event of loss.[537]

As a result, this thesis makes no assertion that the fluctuations of the value of the asset on the blockchain should be attributable to anyone but the individual who holds those assets. These are part of the risk of investment and the focus is instead on liability for faults. The key aspect for this chapter is that the presence of exclusion clauses creates contractual limitations in respect of exchange customers seeking legal redress for systematic errors. The exchanges bear no responsibility for problems in the cryptocurrencies that they list. This renders exchange customers with seemingly very limited legal protection.[538]

It must next be considered whether a claim in negligence could be practical for an exchange customer. The key issue that could limit the practicality of the claim is that the exchange customer will need to prove fault on the part of the exchange to have a successful claim. Within the tort of negligence, if the defendant has acted reasonably, it may be said that they have not breached their duty of care. The standard expected is comparable to the standard of a reasonably competent party that undertakes the particular task.[539] For example, the learner driver would be judged against the standard of a reasonably competent driver when in charge of the motor vehicle.[540] Therefore, an exchange is likely to be judged against the standard of a reasonably competent cryptocurrency exchange. Consequently, if an exchange has used reasonable care and

[536] Saul Levmore, 'Rethinking Ponzi-Scheme Remedies in and out of Bankruptcy' (2012) 92 BU L Rev 969, Pages 970-971.
[537] Financial Conduct Authority (n 113), Page 12.
[538] Ibid, Page 16.
[539] *Nettleship* v *Weston* [1971] 2 QB 691.
[540] Ibid.

skill in their security arrangements then they may not be deemed negligent if, for example, a hack occurs owing to a software error.

Factors such as the foreseeability of risk;[541] the cost of precaution[542] and the social value of the activity[543] can all impact the extent of the standard of care to be expected. In respect of the potential severity of risk, one argument here is that financial risk is not treated with as much caution from a legal perspective in comparison to physical damage.[544] Whilst the level of usage is currently low and so is the risk, the potential risk of impact to the public will increase as usage increases. This has been acknowledged in the latest consultation paper by the UK government with the intent to provide an agile approach to regulatory intervention for risks that may pose a threat to financial stability.[545] With there already being clear threats of scams,[546] hacks,[547] poor governance,[548] possibilities of insider dealing and problems of the DAO,[549] one could argue that risk may occur more regularly if usage increases which then may necessitate further legal control if such levels of risk impact the economy more broadly.[550]

[541] *Bolton* v *Stone* [1951] AC 850.
[542] *Latimer* v *AEC Ltd* [1953] AC 643.
[543] *Watt* v *Hertfordshire County Council* [1954] 1 WLR 835.
[544] Witting (n 484), Page 45; Lee and Ng (n 508), Page 143; *Spartan Steel & Alloys Ltd* v *Martin & Co (Contractors) Ltd* [1973] QB 27.
[545] HM Treasury (n 120), Pages 10-11.
[546] For some examples see, Wilson (n 38); Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368. It is also relevant to note that further regulation and more developed approaches are being applied in this field more broadly but unpermissioned blockchain technology specifically has not been the focus of legal intervention.
[547] For useful summaries of some of the key hacks of exchanges, see Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368.
[548] George Calhoun (forbes.com), 'FTX and ESG: A Panorama of Failed Governance (Pt 1 – The Internal Failures)' (November 2022) <https://www.forbes.com/sites/georgecalhoun/2022/11/21/ftx-and-esg-a-panorama-of-failed-governance-pt-1--the-internal-failures/> Accessed 1st February 2023.
[549] Brian Sanya Mondoh and others, 'Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion?' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144753> Accessed 1st February 2023; Peder Ostbye, 'Exploring The Role of Law in The Governance of Cryptocurrency Systems and Why Limited Liability DAOs might be a Bad Idea' (January 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007547> Accessed 1st February 2023.
[550] HM Treasury (n 120), Pages 10-11.

In respect of the cost of precaution, claims are likely to fail if the precautions taken were reasonable and further precautions would have been disproportionally expensive.[551] It could hardly be argued that the cost of precaution in respect of the security of the exchange would be disproportionally expensive when it could be regarded as a necessity for the running of the exchange itself. Although claims would likely fail, providing the exchange takes reasonable precautions. Furthermore, the need for precautions can be mitigated by emergency circumstances as seen in the *Watt*[552] case, although there is still the requirement of relevant diligence.[553] In the context of crypto, the social value of cryptocurrency trading is not equitable to matters of life and death and so would not prevent a sufficient standard from being set. Whilst these factors may not mitigate the standard of care expected by exchanges, it is important to note the multitude of factors that can impact the assessment of reasonableness and the particular standard that they will be held to.

The assessment of the particular circumstances and the "reasonableness" of a party has been discussed in the context of cybersecurity in the United States, where it has been stated that "legal compliance with current U.S. cybersecurity law relies heavily on interpreting and implementing 'reasonable' and 'appropriate' cybersecurity measures.[554] In the UK, there can be regarded as a fine balance between protecting the exchange customer in this context, and not over-burdening the exchange by imposing a standard of care that is not within the industry norm.[555]

It is worth also mentioning that there has been a reluctance from courts to uphold negligence claims against exchanges and impose a liability that extends beyond

[551] *Latimer* v *AEC Ltd* [1953] AC 643.
[552] *Watt* v *Hertfordshire County Council* [1954] 1 WLR 835.
[553] *Ward* v *London County Council* [1938] 2 All ER 341.
[554] Scott Shackleford and others, 'Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices' (2015) 50(2-3) Texas International Law Journal 305, Page 340.
[555] Ibid, Page 347.

their contractual agreement.[556] This is exemplified in the American legal system with an example such as *Berk*[557] whereby claimants tried to frame their claim in negligence for the losses they suffered as a result of Coinbase's launch of Bitcoin Cash which the claimants stated should have been managed differently. Ultimately, the court in *Berk* stated that it was a contractual interpretation issue and not a negligence one.[558] The exchange included an arbitration clause, so the court said that arbitration was the correct dispute resolution medium and therefore it did not deal with the negligence claim.[559]

An additional case worth noting is the case of *BMA LLC*[560] whereby claimants alleged negligence of BitMEX (amongst other claims) for not following financial regulations and anti-money laundering checks as well as accusations of trading in opposition to the customers.[561] Ultimately the courts rejected claims of negligence by saying the claimants had failed to show the existence of a special relationship between themselves and BitMEX which should give rise to a duty of care.[562]

The final US case worth noting here is *Shin*[563] whereby after a series of events, the investors ICX assets were frozen by ICON who stated that there had been a malicious attack.[564] The investor (Shin) launched a series of legal claims in relation to this, one of which was under the parameters of tort and yet all claims failed.[565] In relation to the prima facie tort claim under Colorado law, the courts effectively denied this because no prior case law could support such a finding.[566]

---

[556] Robert Schwinger, 'Blockchain Law: When plaintiffs raise claims of platforms behaving badly' (July 2021) New York Law Journal <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/blockchain-law---when-plaintiffs-raise-claims-of-platforms-behaving-badly.pdf?revision=3fe041d8-c2d6-42f9-913b-0b21c7f53b17&revision=3fe041d8-c2d6-42f9-913b-0b21c7f53b17> Accessed 1st February 2023.
[557] *Berk* v *Coinbase* 840 Fed Appx 914, (9th Cir, 23rd December 2020) (not for publication) rev'g 2019 WL 3561926 (ND Calif 6th August 2019).
[558] Ibid; Schwinger (n 556).
[559] Ibid.
[560] *BMA LLC* v *HDR Global Trading Ltd* 2021 WL 949371 (ND Calif 12th March 2021).
[561] Ibid, Section I.
[562] Ibid, Section IV-C.
[563] *Shin* v *ICON Found* 2021 WL 1893117 (ND Calif 11th May 2021).
[564] Ibid, Pages 726-727.
[565] Ibid, Page 737.
[566] Ibid, Pages 736-737.

Whilst these cases may be settled differently under English law, the key principles taken here are how difficult claims against exchanges may be in tort where the contractual agreement has not been breached and that it may be that cases could end up in arbitration rather than going to court. The difficulty of a tortious claim in this context will be further highlighted in the following discussion.

The standard of care that is to be provided by an exchange may differ depending on the service that the exchange offers. Usually, cryptocurrencies are to be held in a virtual wallet. Some exchanges provide such a wallet service to their customers, normally in return for monthly payments in the form of a subscription. Some exchanges do not provide this service and merely provide access to the cryptocurrencies to be stored in the customer's wallet that they may have through a third party.[567] It is worth mentioning that there may be a possibility to explore whether exchanges have a fiduciary duty to segregate the relevant amounts of cryptocurrency when providing the wallet service and, if they do not do so and cannot meet any claims arising out of wallet theft, whether fiduciary liability could arise. A key aspect here would be whether there can truly be said to be a relationship of trust and confidence between the exchange customer and the exchange.[568] The FCA's warning of the risk associated with cryptocurrencies,[569] the number of hacks,[570] and publicised issues with exchanges[571] could suggest that exchange customers should not have this degree of trust and

[567] For a brief discussion of the threat of wallet theft, see UK Government Chief Scientific Adviser (n 237), Page 12.
[568] For an interesting discussion on trust and confidence and the concept of fiduciary duty in blockchain and decentralised platforms see, Balazs Bodo and Primavera De Filippi, 'Trust in Context: The Impact of Regulation on Blockchain and DeFi' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051842> Accessed 1st February 2023.
[569] Financial Conduct Authority, 'FCA warns consumers of the risks of investments advertising high returns based on cryptoassets' (January 2021) <https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets> Accessed 1st February 2023.
[570] For useful summaries of some of the key hacks of exchanges, see Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368.
[571] For a discussion on FTX see, Calhoun (n 548).

confidence in the exchanges and should be aware that it is a risky investment. Although potentially storing assets with the exchange could suggest trust and confidence in them. The *Tulip Trading*[572] case would suggest that it would be unlikely for such a relationship to amount to a fiduciary duty under the present approach of the common law although matters would be determined on the facts of the case and there is potential for specific circumstances to give rise to a fiduciary duty.[573] Whilst it remains a possibility for the case law to develop and find the circumstance in which the exchanges owe a fiduciary duty to its exchange customers, it appears unlikely that this could extend to systematic errors which occur on the underlying blockchain, providing it is truly decentralised and the exchange has no such control over it. As has been stated previously, further exploration of fiduciary duty is beyond the scope of the focus here but does highlight the potential differing standards that exchanges may be held to.

It may be said that exchanges are not required in tort to ensure the security of the exchange and its customers' investments. Instead, the standard that is likely to be imposed is a reasonable attempt at providing security. This standard is likely to be set and compared against a reasonable cryptocurrency exchange.[574] Therefore, where an exchange invests in the security by utilising similar security software and coding or by spending a similar financial amount on security to that of a reasonable cryptocurrency exchange, then it may be said that such an exchange has met its standard of care and not breached its duty in respect of the security to their exchange customers. Training of the staff may also be a relevant practice in this context as this can be an essential security

[572] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624.
[573] Ibid, Para [97]; *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16, Paras [41], [86] and [91].
[574] *Vaughan* v *Menlove* (1837) 132 ER 490.

measure to prevent cybersecurity mistakes from happening.[575] This would be so, irrespective of whether a hack, for example, occurs.

Although each case could depend on the particular facts, where an exchange acts reasonably by monitoring and updating their security to the industry standard, then they would not be deemed negligent even if an error were to occur. Therefore, no legal protection would be derived from any losses the exchange customer suffers providing the exchange was a reasonable exchange. This threshold of liability would not necessarily incentivise exchanges to invest further to seek to guarantee enhanced protections for their exchange customers. Arguably one of the most prominent examples of negligent management of a cryptocurrency exchange can be seen in the hack of Mt. Gox.[576] The security coding in the exchange was highly outdated and would be an example of when an exchange could be said to have fallen below the standard of a reasonable exchange. In 2014, the mismanagement of what was at the time an industry-leading exchange resulted in nearly half a billion dollars' worth of Bitcoin being stolen, which resulted in Federal investigations and numerous lawsuits.[577] Whilst the exchange's standards did fall below the standard expected and resulted in legal ramifications, it could be argued that generally the most compelling incentive for exchanges to seek to ensure security of their exchange is the threat to their reputation should a hack occur.[578]

Therefore, this section has indicated that although the presence of the exchange as an intermediary can provide a potential defendant to be pursued,[579] the exchange

[575] Rebecca Parry, 'Building A Legal Framework to Facilitate The Transformative Potential of Digital Economies' (2022) 10 NIBLeJ 5 <https://www.ntu.ac.uk/__data/assets/pdf_file/0039/1849890/2022-10-NIBLeJ-5.pdf> Accessed 1st February 2023, Page 12.
[576] For more insight into this story see, Robert McMillan (Wired.com), 'The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster' (2014) <https://www.wired.com/2014/03/bitcoin-exchange/> Accessed 1st February 2023.
[577] Yoshifumi Takemoto and Sophie Knight (Retuers.com) <https://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228> Accessed 1st February 2023; Ibid.
[578] Ostbye (n 202), Page 18.
[579] Ibid, Page 17.

would likely not bear legal liability if they adopted the standards of a reasonable exchange and may only be liable if they acted negligently. The relationship between the exchange and the exchange customer is contractual but the terms and conditions of service restrict liability of the exchange to the extent that negligence is required.[580] This limits the practicality of contract law as an avenue for redress for losses derived from systematic errors for exchange customers. Within tort law, there are problems of the standard of care expected for issues such as the security of the exchange and any imposition of a fiduciary duty on the exchange will be assessed on the facts of the case but seems unlikely.[581] Consequently, it appears that where an exchange follows the industry standard and acts reasonably, no liability shall befall them irrespective of any losses incurred by exchange customers resulting from systematic errors. Arguably, the threat of damage to reputation may therefore be a greater incentive for the exchanges to protect the exchange customer than threat of liability for systematic errors.[582]

4.2.3: DeFi

Within the cryptocurrency market, some exchanges themselves have become decentralised and are referred to as DeFi exchanges (also known as DEXs).[583] The DeFi or DEX customers transact on a peer-to-peer basis and are therefore in a different position to general exchange customers discussed above. These DEXs normally operate on the Ethereum blockchain.[584] DeFi exchanges raise interesting issues of liability for systematic errors within unpermissioned blockchain technology.

In traditional exchanges, the contract is formed between the exchange customer and the exchange. Whilst liability is often restricted as highlighted previously, there is

[580] For an example, see binance.com (n 203), Part IV Sections 2-3.
[581] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624, Para [97].
[582] Ostbye (n 202), Page 18.
[583] Johnstone (n 101), Page 169; Vijay Mohan, 'Automated Market Makers and Decentralized Exchanges: A DeFi Primer' (2022) 8 Financial Innovation, Article 20, Page 1.
[584] Vijay Mohan, 'Automated Market Makers and Decentralized Exchanges: A DeFi Primer' (2022) 8 Financial Innovation, Article 20, Page 4.

still a recognisable party in the exchange that the exchange customer could potentially pursue if it is negligent. "A DEX provides agents with the opportunity to exchange one asset for another without a centralized third-party responsible for overseeing trading activity."[585] It has also been referred to as "atomic swaps" whereby the swap will only happen once both parties have agreed to release their cryptocurrency.[586] Purchasing cryptocurrency through decentralised exchanges will further inhibit the legal protection afforded to the users within this market, compared with centralised exchanges. This is due to the potential lack of a central party which can limit the enforceability of contract law.

The hacks of centralised exchanges such as Mt. Gox and the potential for significant reward for everyday investors in utilising these crypto-swaps may have contributed to the surge in the use of these DeFi platforms. Some figures suggest that the volume of users interacting with DeFi platforms such as DEXs has increased three thousand eight hundred percent between the beginning of 2020 and the end of 2022 and that DEX trading amounting to eight hundred and fifty four billion dollars in 2022 alone.[587] The incentive to invest in these DeFi platforms is only exacerbated by the "historically low or sub-zero interest rates".[588] However, DeFi or DEXs are not free from such systematic errors also.[589] In August 2021 a DeFi platform was hacked and had over six hundred million dollars' worth of cryptocurrency stolen.[590] Some estimates suggest that such hacks of DeFi platforms in 2021 alone totalled over ten billion dollars.[591] More recently, the secretary-general of the International Organization of

[585] Ibid, Page 3.
[586] Ostbye (n 323), Page 9.
[587] Nansen.ai (n 39). This is a significant increased from previous years with figures suggesting that the money placed into DeFi platforms including DEXs increased from twelve billion dollars in 2020 to approximately eighty-six billion dollars in 2021. For these earlier figures see, Wilson (n 38).
[588] Wilson (n 38).
[589] Ibid.
[590] Wilson and Westbrook (n 200).
[591] Wilson (n 38).

Securities Commissions (IOSCo) has acknowledged that there are a number of concerns within the DeFi markets and its current rate of growth creates a need for "closer attention by regulators".[592]

It is therefore apparent that systematic errors are present within this new strand of DeFi platforms. DEXs seem to almost be a hybrid between the traditional peer-to-peer model and the exchange-based model. There can be a company that oversees the operation in DeFi platforms, but they still use the decentralised blockchain to enable it to take place.[593] Parties can trade cryptocurrency on a peer-to-peer basis, in comparison to traditional exchanges whereby customers buy cryptocurrency using fiat currency.[594]

Whilst theoretically the DEX enables decentralised trading and utilises smart contracts to enable peer-to-peer trading to occur, power is often retained by the DEX themselves as a key component within the smart contract.[595] For example, this power retention was evident in the Curve DEX whereby voting rights for the DEX were largely controlled by the founder of the DEX.[596] This has led to IOSCo warning that some DeFi platforms may be "decentralised in name only".[597]

The organisation that oversees the DEX may therefore provide another potential defendant to be pursued. In a circumstance where a coding error occurs in the DEX which results in a hack, for example, then the fault may be attached to the entity that oversees the DEX. However, their use of the DEX or DeFi platform may remove the

---

[592] Kruppa (n 93).
[593] Celsius, 'Why trust Celsius' <https://celsius.network/why-trust-celsius> Accessed 1st February 2023.
[594] Crypto Renegade, 'Decentralized Exchanges Explained' (2021) <https://www.youtube.com/watch?v=dgr3yAr2nCE> Accessed 1st February 2023, Minutes 0:50-2:20.
[595] For general insight into the operation of DEXs see, Robert Stevens (decrpt.co), 'DeFi: The Ultimate Beginner's Guide to Decentralized Finance' (January 2021) <https://decrypt.co/resources/defi-ultimate-beginners-guide-decentralized-finance> Accessed 1st February 2023.
[596] For further information see, Amy Castor and Daniel Phillips (decrypt.co), 'Curve founder seizes 71% of Curve DAO voting power' (August 2020) <https://decrypt.co/39599/curve-founder-seizes-71-of-curve-dao-voting-power> Accessed 1st February 2023.
[597] Kruppa (n 93). A useful example here can be found in the EtherDelta exchange which operated through smart contracts and utilised a protocol for decentralised exchanges on the Ethereum blockchain but was deemed to constitute an 'exchange' under the SEC remit. For further information see, *United States of America before the Securities and Exchange commission In the Matter of Zachary Coburn*, Release No 84553, File No 3-18888 (8th November 2018) <https://www.sec.gov/files/litigation/admin/2018/34-84553.pdf> Accessed 1st August 2023.

DEX company from the fault of the systematic error which occurs on the blockchain itself. Where an error occurs on the decentralised blockchain itself, it is likely that the same problems within contract and tort could arise. Particularly, in choosing to use a DEX over a traditional exchange, the parties may rely on the immutability of the ledger rather than the traditional legal approaches should fault arise, as is the case in the peer-to-peer network. The presence of the company that oversees the DEX could provide a potential defendant, like that of a centralised exchange. However, any such liability is likely to be restricted significantly. The DEX does not control the blockchain itself but has merely created a platform that runs on it and as discussed in section 3.3.2, often will also include exclusion clauses in their terms and conditions much like traditional exchanges.[598] Therefore, their liability would only extend to coding errors of the DEX platform itself, although such liability would be limited, and no liability could be attached for the underlying principles or errors of the blockchain technology.

This would therefore suggest that presently there is a limited lack of legal protection for systematic errors within unpermissioned blockchain technology. Whether you interact with the technology peer-to-peer, or through trades on a centralised exchange, or on a DeFi platform such as a DEX, the practicality of pursuing a legal claim in contract or tort seems significantly limited. Given the volatility of cryptocurrencies and the warning by the FCA against investment in this sector,[599] it would require a significant policy change if regulators were to provide a greater level of protection for users in cases where there are systematic errors within unpermissioned blockchain technology. The recent consultation paper states that such a policy change

[598] Celsius, 'Customer Care' <https://celsius.network/customer-care> Accessed 1st February 2023; (dydx.com), 'Terms of Use' (February 2023) <https://dydx.exchange/terms?> Accessed 1st February 2023, Paras 10-11; (uniswap.org), 'Uniswap Labs Terms of Service' (November 2022) <https://uniswap.org/terms-of-service> Accessed 1st February 2023, Assumption of Risk-Indemnity; (docs.kine.im), 'Terms of Use' (February 2021) <https://docs.kine.im/library/terms-of-use> Accessed 1st February 2023, (1)-(3).
[599] Financial Conduct Authority (n 569).

would only be likely where market integrity is impacted or there is a threat of macroeconomic instability, which the current level of usage in the UK market does not suggest is likely in the near future.[600] The development of redress is likely to remain in the hands of the courts as cases are brought and the law will evolve if remedies are appropriate.

4.3: Conclusion

Currently, English law does not provide adequate legal redress for systematic errors within unpermissioned blockchain technology in contract or tort. Within the peer-to-peer model of unpermissioned blockchain, the presence of anonymity[601] and the lack of intention to be legally bound[602] may inhibit a legal claim being made in contract law by peer-to-peer users. Within tort law, a further two problems could limit the practicality of a legal claim and are highlighted in the *Tulip Trading* case, although that case so far was only concerned with whether or not there was a triable issue.[603] The lack of a clear hierarchical structure means it can be difficult to apportion a standard of care to a specific role within unpermissioned blockchain technology.[604] Furthermore, unless loss of cryptocurrency is viewed as property damage the loss suffered is likely to be purely economic, which is generally unrecoverable in English tort law.[605]

[600] HM Treasury (n 120), Pages 8-11.
[601] Houben (n 60), Page 263; Sage (n 451), Page 473; See also the discussion in 2.2.
[602] Ghosh (n 460), Chapter 34, Page 1; Gregory Klass, 'Intent to Contract' (2009) 95 Va L Rev 1437, Page 1439; Dori Kimel, *From Promise to Contract: Towards a Liberal Theory of Contract* (Bloomsbury 2003), Pages 136-139.
[603] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624.
[604] David Capps and Fraser Collingham, 'High Court decided on first English law case on crypto software duties' (April 2022) <https://www.lexology.com/library/detail.aspx?g=a6a60e6f-d365-45d3-bb99-3bdf505883ce> Accessed 1st February 2023; *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624, Paras [97-100]; UK Government Chief Scientific Adviser (n 237), Page 5.
[605] *Tulip Trading Ltd* v *Bitcoin Association For BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624, Para [86]; David Capps and Fraser Collingham, 'High Court decided on first English law case on crypto software duties' (April 2022) <https://www.lexology.com/library/detail.aspx?g=a6a60e6f-d365-45d3-bb99-3bdf505883ce> Accessed 1st February 2023; Lee and Ng (n 508), Page 143.

In the exchange-based transactions, the presence of an intermediary provides a potential identifiable defendant in such claims.[606] However, in the traditional exchanges, exclusion clauses limit the possibility of such claim being brought and they would not provide protection against faults with the underlying blockchains on which cryptocurrencies operate. Therefore, the threat to the reputation of the exchange may be greater than the threat of a liability claim.[607]

Furthermore, blockchain technology is still evolving and the rise in presence of DeFi platforms such as DEXs has further complicated the legal landscape for liability within this area.[608] The potential for systematic errors such as fraudulent trading or hacking is as present within the DEX model as it is in the exchange-based or peer-to-peer models.[609] The organisation that oversees the DEX theoretically provides another potential defendant to be pursued, as if coding errors occur in the DEX leading to hacking, for example, then the fault may be attached to the company that oversees the DEX. However, their use of the DEX or DeFi platform also can further remove themselves from the fault of the systematic error, where such fault occurs on the blockchain itself.

The courts have displayed a willingness to expedite proceedings or not alert potential defendants in an attempt to assist victims of fraud in unpermissioned blockchain technology. [610] However, this approach relies heavily on international cooperation and so may not necessarily provide a consistently practical form of legal redress for systematic errors in unpermissioned blockchain technology.[611] The

[606] Ostbye (n 202), Page 17.
[607] Ibid, Page 18.
[608] Wilson and Westbrook (n 200), Page 1.
[609] Ekin Genc and Stephen Graves, '13 Biggest DeFi Hacks and Heists' (April 2022) <https://decrypt.co/93874/biggest-defi-hacks-heists> Accessed 1st February 2023; Wilson (n 38); Wilson and Westbrook (n 200).
[610] Collyer Bristow (n 272), Minutes 45-47; *Fetch.ai Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm), [2021] WLUK 601*.
[611] Collyer Bristow (n 272), Minutes 49-51.

consequence is that although some users of unpermissioned blockchain technology may have the possibility of a legal claim within English law, practically there is limited legal protection irrespective of the model of access used for the unpermissioned blockchain (peer-to-peer, exchange, or DEX). This is one risk that is faced by investors in cryptocurrencies, many of whom are consumers, and it is also notable that there can be poor governance in these investments as seen with the circumstances of Terra/Luna.[612] It has therefore become apparent that if regulators wish to provide further protection in the form of legal redress, a policy change may be needed.[613]

As blockchain technology continues to develop, the regulatory framework is also likely to evolve. Whether this is through various policy choices discussed in the following chapter,[614] regulation, self-regulation,[615] or the creation of a new subset of law in the form of *Lex Cryptographia*,[616] regulators are faced with a choice to determine their approach if further protection is sought. Whether regulators desire such a change or not will become clearer over the coming years, however, the rise in scams could suggest an increased need for protection from systematic errors within unpermissioned blockchain technology.[617] The following chapter will therefore explore potential policy choices and whether regulation is justified for systematic errors. Additionally, based on the principles of Ostrom,[618] whether unpermissioned blockchain technology may be regarded as self-governing or capable of self-regulating to understand the practical options available if further protection is sought.

---

[612] For a discussion on Terra/Luna see, Q.ai (forbes.com), 'What Really Happened To LUNA Crypto' (September 2022) <https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=68ff269a4ff1> Accessed 1st February 2023.
[613] Chiu (n 100), Page 271.
[614] Ibid, Page 263.
[615] Yeung (n 254), Page 209.
[616] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> Accessed 1st February 2023, Page 4.
[617] Peter Yeoh, 'Regulatory issues in blockchain technology' (2017) 25(2) Journal of Financial Regulation and Compliance 196, Page 202.
[618] Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press 1990).

Chapter 5: Normative Evaluations. Is There the Need for Legal Intervention, or Is Unpermissioned Blockchain Technology Already Adequately Self-Regulated with respect to Systematic Faults?

5.1: Introduction and context

Chapter 4 highlighted that contract and tort are unlikely to provide practical forms of legal redress to the end users within unpermissioned blockchain technology for losses derived from systematic errors. Therefore, if further legal protection of peer-to-peer users, exchange customers and DEX customers is sought, a novel approach may need to be considered. This chapter will seek to determine the potential of regulation for protecting these end users. Such an approach would address the risk presented by a lack of redress for faults in the underlying blockchain, but also other risks presented by unpermissioned blockchain technology, notably cryptocurrencies. It is important to acknowledge the work of Karen Yeung[619] as it helps to shape some of the key questions and contributions of this chapter. Yeung analyses whether blockchain will avoid conventional regulation.[620] The concept of "conventional regulation", in the form of state control, will be examined in section 5.2.1. Therefore, the question posed by Yeung is if blockchain is capable of evading state control. This chapter will explore this idea further and will build on Chiu's discussion of regulatory options,[621] as well as Black's concept of regulation.[622]

The current English regulatory approach to losses suffered by end users due to systematic errors, as well as other risks, within unpermissioned blockchain technology has been to warn of the risks and acknowledge the limited legal protection afforded.[623]

[619] Yeung (n 254).
[620] Ibid, Page 207.
[621] Chiu (n 100), Page 263.
[622] Julia Black, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1, Page 26.
[623] Financial Conduct Authority (n 569).

An intention to introduce more stringent regulation has been announced more recently.[624] Even under the consultation proposals however, there is limited scope for practical legal redress irrespective of the method of transaction chosen. In the peer-to-peer method, issues of anonymity and doubts about jurisdiction may limit claims. In cases involving exchanges, exclusion clauses limit liability to the point of negligence and in the context of DEX, all the above issues may be present depending on the nature of the DEX itself. Regulation can offer potential for greater legal redress; however, it can be a lengthy and costly process.[625]

This chapter will therefore explore the meaning and legitimacy of regulation in its application to unpermissioned blockchain technology to determine when regulation may be applied.[626] It will consider Black's model of regulation, as well as Chiu's discussion of regulatory choices. Under Black's approach self-regulation would be a possibility. Further to this, Ostrom's self-management theory will be explored in the context of unpermissioned blockchain technology to determine the possibility of self-regulation for peer-to-peer transactions on Ostrom's model. Although Ostrom's theory is focused on the preservation of a natural resource,[627] such principles can be translated into unpermissioned blockchain technology as an analogy of the potential to self-manage.[628] Natural resources and unpermissioned blockchain technology are both unique, often limited in quantity[629] and are not necessarily created or controlled by a

[624] HM Treasury (n 120), Pages 7-12.
[625] Andrei Shleifer, 'Understanding Regulation' (2005) 11(4) European Financial Management 439, Pages 440-441.
[626] Baldwin, Cave and Lodge (n 62), Page 2.
[627] See the discussion surrounding the various stories about threats to our natural resources Ostrom (n 618), Page 1.
[628] For an interesting discussion on 'self-management' within decentralised platforms see, Chiu (n 100), Pages 295-297 and also pages 262, 280, 284 and 288.
[629] One example could be Bitcoin, which uses unpermissioned blockchain technology and is limited in number. Additionally, due to the complexity of its validation process, there could be said to be a limit on the speed and processing power within unpermissioned blockchain technology. This is further exemplified by the operation of unpermissioned blockchain technology being highly incentivised with no 'obligation' to 'mine' or 'validate'.

central agency.[630] Ostrom informs the debate of whether unpermissioned blockchain technology is capable of some degree of self-regulation in how liability for faults is allocated,[631] although ultimately the difficulties of such an approach will be highlighted.

5.1.1: An overview of regulation theory

Regulation is a legal device than can positively or negatively impact all aspects of society.[632] Consequently, it must be treated as a potential option but not the go-to solution for every legal, societal or economic issue that could arise.[633] The modern[634] process of regulation focuses on social behaviours, the value of risk and the morality of society.[635] This may fit more suitably to unpermissioned blockchain technology rather than the traditional approach of strict legal rules with punishment as a consequence for breaches.[636] In applying this broader, socio-political view of regulation to

[630] A common approach for the management of natural resources is that of a centralised agency. The discussion here is that nobody 'naturally' owns or controls a natural resource. There is similarity to unpermissioned blockchain technology in the lack of centralisation.
[631] See sections 5.5 and 5.6 respectively; Ostrom (n 618), Pages 91-101.
[632] For a brief summary of some positives and negatives of regulation see, JL Porket, 'The Pros and Cons of Government Regulation' (2003) Institute of Economic Affairs 3rd discussion paper <https://iea.org.uk/wp-content/uploads/2016/07/upldbook341pdf.pdf> Accessed 1st February 2023.
[633] For an interesting summary of how regulation impacts our daily lives and the key questions that must be considered in regulation as a topic see, Shleifer (n 625), Page 439.
[634] Regulation has developed over time both as a theory and in its usage. See Baldwin, Cave and Lodge (n 62), Page 2. A factor such as globalisation could be said to have stimulated the rise in regulation to some extent. See Baldwin, Cave and Lodge (n 62), Pages 4-5; Black (n 622), Page 1.
[635] Baldwin, Cave and Lodge (n 62), Page 9. For some discussions on the impact of economics, sociology and psychology on the law, see Alfred Kahn, 'The Economics of Regulation: Principles and Institutions' (2012) <https://www.bcuc.com/Documents/Proceedings/2012/DOC_29762_A2-28_Submission.pdf> Accessed 1st February 2023; Regine Paul and others (eds), *Society, Regulation and Governance: New Modes of Shaping Social Change?* (Edward Elgar Publishing 2017), Page 2; Omer Lee Reed Jr, 'The Psychological Impact of TV Advertising and the Need for FTC Regulation' (1975) 13 Am Bus LJ 171 respectively.
[636] Baldwin, Cave and Lodge (n 62), Pages 2-3. For some discussion of some of the limitations of the traditional view of regulation see, Ian Ayers and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992), Page 5.

unpermissioned blockchain technology, we can appreciate a broader scope of solutions for the lack of legal redress for systematic errors. [637]

5.2: What is "regulation"?

Regulation is commonly viewed through the command-and-control perspective whereby the state sets strict rules and utilises the threat of punishment as a deterrent for breaching such rules.[638] The command-and-control approach will be explored in the following section. The second view of regulation that will be explored is the meaning of regulation that is relied upon for the thesis,[639] which is Julia Black's "decentred regulation".[640]

[637] "Regulatory agencies will be able to speak more softly when they are perceived as carrying big sticks." (See, Ian Ayers and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992), Pages 5-6). This highlights that regulators must have a variety of sanctions available to them. By showing a willingness to escalate to a higher sanction, theoretically society will be more compliant. Society is more likely to accept regulation if there is the possible threat of a tougher sanction. This could be because the regulator is perceived as fair where they do not use the most intrusive form of regulation. This further enhances the potential benefits of adopting the decentred perspective of regulation which encompasses more 'regulatory options' than the traditional approach.

[638] Jingxiao Zhang and others, 'The impact of environmental regulations on urban Green innovation efficiency: The case of Xi'an' (2020) 57 Sustainable Cities and Society, Article 102123, Page 2; Black (n 622), Page 2.

[639] Some regulatory theories will not be discussed in this chapter but were considered and will be explained briefly here. For example, public interest theory is founded on the concept of a market and a presumption that it will fail. Market failure will be discussed in this chapter, so the theory is not worth further consideration. Private interest theory seems applicable to unpermissioned blockchain technology. The approach relies on a 'free market' concept, it produces a more relaxed approach to regulation. This could be likened to the current approach of the UK towards the peer-to-peer model of unpermissioned blockchain technology although it is not clear whether this may change if further risk manifests. See, Financial Conduct Authority (n 113), Page 12. Additionally, the 'regulatory space' theory indicates the possibility of different entities filling the regulatory role which can be applicable to unpermissioned blockchain technology through concepts such as 'code as law'. For further discussion see, Terrence Daintith, 'A Regulatory Space Agency' (1989) 9(4) Oxford Journal of Legal Studies 534, Page 543; Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, 2007), Page 59; Leigh Hancher and Michael Moran, *Organizing regulatory space* (1989) as found in Robert Baldwin, Colin Scott and Christopher Hood, *A reader on Regulation* (Oxford University Press 1998), Page 153. The final theory is systems theory. This shows how the novel nature of unpermissioned blockchain technology may be incompatible with legal and societal systems which suggests that a careful balance is needed, and that self-regulation can be explored. For further understanding see, Gunther Teubner ed, *Juridification of Social Spheres: A Comparative Analysis of Labor, Corporate, Antitrust and Social Welfare Law* (Walter de Gruyter 2012), Pages 22-26; Ana Lourenco, 'Autopoietic Social Systems Theory: The Co-evolution of Law and the Economy' (2010) Working Paper No 409 Centre for Business Research, University of Cambridge <https://www.cbr.cam.ac.uk/fileadmin/user_upload/centre-for-business-research/downloads/working-papers/wp409.pdf> Accessed 1st February 2023, Page 2.

[640] See section 5.2.2; Black (n 622), Page 26. For a critique of this theory see, Dimity Kingsford Smith, 'What is Regulation – A Reply to Julia Black' (2002) 27 Australian Journal of Legal Philosophy 37.

5.2.1: The "central meaning"

"The core understanding that many have of 'regulation' is some form of 'command-and-control' (CAC) regulation: regulation by the state through the use of legal rules backed by (often criminal) sanctions."[641] This suggests that the common understanding of regulation is perceived as purely unilateral governmental activity, "governments telling, [and] others doing".[642] This suggests that the state is best-placed to understand the views of society and protect them from the harm that would arise from a free market which may create a paternalistic approach.[643] Direct state control would be difficult to achieve satisfactorily in relation to unpermissioned blockchain technology. Regulation within the "central meaning" would need to provide clear and defined rules, targeting specific parties to be effective. However, due to the lack of a centralised party,[644] the nature of the supranational[645] technology and the potential for anonymity within the peer-to-peer model, [646] regulation as informed by the central meaning is highly unlikely.[647] Clear rules regarding modern technologies would also be likely to

[641] Black (n 622), Page 2. Selznick's definition would be another example of a definition within the 'central meaning'. See Baldwin, Cave and Lodge (n 62), Pages 2-3. For a discussion on the potential efficiency of the command-and-control approach see, Daniel Cole, 'When is Command-and-Control Efficient? Institutions, Technology, and the Comparative Efficiency of Alternative Regulatory Regimes For Environmental Protection' (1999) Wisconsin Law Review 887.
[642] Black (n 622), Page 3. Context and culture can impact the interpretation of regulation to include activities which are not purely governmental. However, the common understanding of regulation is governmental activity. See Anthony Ogus, *Regulation: Legal Form and Economic Theory* (Clarendon Press 1994), Page 1.
[643] Anthony Onus, *Regulation: Legal Form and Economic Theory* (Clarendon Press 1994), Chapter 3. For an interesting discussion of how some state involvement may still be an essential aspect of regulation see, Rebecca Schmidt and Colin Scott, 'Regulatory discretion: structuring power in the era of regulatory capitalism' (2021) 41 Legal Studies 454.
[644] Financial Conduct Authority (n 113), Page 23.
[645] Bjelajac and Bajac (n 54), Page 22.
[646] Houben (n 60), Page 263.
[647] The only examples of regulation that may fall under this central meaning would seemingly be outright bans. Numerous countries have adopted approaches towards Bitcoin for example that effectively amounts to a ban.

become out of date swiftly. As a result, this "central meaning" of regulation does not seem very beneficial for application to unpermissioned blockchain technology.[648]

Morgan & Yeung highlight that the "central meaning" is founded on three assumptions that lack support. Assumption 1 is that the state is best suited to understand community interests. Morgan & Yeung acknowledge that in modern society, non-state bodies have the capability to understand community interests better than the state.[649] Assumption 2 is that the state is always the highest form of authority. Morgan & Yeung suggest that multi-faceted forms of governance exist.[650] In applying these points to unpermissioned blockchain technology, it could be said that the state will always have an overarching regulatory power but the state may also choose if it wishes to regulate or to leave the entities within unpermissioned blockchain technology to self-regulate through coding.[651] This is a concept that will be explored further under Julia Black's decentred regulation idea.[652] Assumption 3 is that command rules operate as the most effective form of behaviour modification.[653] Morgan & Yeung highlight that command rules are not perceived positively 100% of the time and it may be the case with those involved in digital technologies.[654]

[648] There exists some indirect regulation within unpermissioned blockchain technology, but not for the context of systematic errors. For example, countries often regarded as 'banning Bitcoin', do not have an outright ban on the currency itself, but utilise heavily restrictive laws to make it a highly impractical asset. One example can be seen in China, whereby they have regulated heavily exchanges and miners rather than a prohibition on Bitcoin. For further discussion see, John Riley, 'The Current Status of Cryptocurrency Regulation in China and Its Effect around the World' (2021) 1 China & WTO Review 135.
[649] Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, 2007), Page 4.
[650] Ibid. This is also present in Prosser's second vision of regulation. For more discussion on this see, Tony Prosser, 'Two visions of Regulation: Paper for 'Regulation in the Age of Crisis' (2010) <http://regulation.upf.edu/dublin-10-papers/1H1.pdf> Accessed 1st February 2023, Page 6.
[651] Tony Prosser, 'Two visions of Regulation: Paper for 'Regulation in the Age of Crisis' (2010) <http://regulation.upf.edu/dublin-10-papers/1H1.pdf> Accessed 1st February 2023, Page 6.
[652] See section 5.2.2; Black (n 622), Page 26.
[653] Gunther Teubner ed, *Juridification of Social Spheres: A Comparative Analysis of Labor, Corporate, Antitrust and Social Welfare Law* (Walter de Gruyter 2012), Pages 22-24.
[654] Chris Reed, 'Why Judges Need Jurisprudence in Cyberspace' (2018) 38 Legal Studies 263, Pages 265-267.

Over-reliance on this command-and-control approach to regulation, can lead to regulatory failure in that the regulation may not be effective for its purpose.[655] Ayers and Braithwaite suggest that states must retain an "oversight function"[656] and that it may be regarded as being more important now than ever.[657] Strict adherence to command-and-control rules as a method of intervention can create a rigid and impractical structure as a means of regulatory intervention.[658] Instead, Ayers & Braithwaite suggest that such rules can be considered or even eventually used when necessary, but instead that alternatives should be pursued initially.[659]

Practically there exist a significant number of alternatives for regulation other than command-type rules.[660] Consequently, as will be seen in the discussion below of policy choices and decentred regulation, a broader and more contextually aware view of regulation would be more practical especially with a technological development such as unpermissioned blockchain technology.[661]

---

[655] For some discussion of the type of regulatory failure that can occur, see Black (n 622), Page 3. For further discussion of regulatory failure that can occur in the Banking sector when considering global governance aspects see, Roman Goldbach, *Global Governance and Regulatory Failure: The Political Economy of Banking* (Palgrave Macmillan 2015).

[656] Ian Ayers and John Braithwaite, 'Responsive Regulation: Transcending the Deregulation Debate', in Martin Lodge, Edward Page and Steven Balla (eds), *The Oxford Handbook of Classics in Public Policy and Administration* (Oxford University Press 2015), Page 559.

[657] Ibid.

[658] Ibid, Page 561.

[659] Ibid, Page 572.

[660] Morgan and Yeung (n 649), Page 4. One example of a different approach to command-and-control would be regulation for the purpose of information disclosure. Regulation can be used merely to ensure that certain information is made available freely in the market. Most commonly, this technique is for the benefit of consumers. One example within unpermissioned blockchain technology, can be seen in the requirement of registration for UK cryptoasset businesses with the Financial Conduct Authority. This is to protect consumers and limit money laundering possibilities. For more information on such a registration requirement, see Financial Conduct Authority (n 511). For more information on the issues of regulation for the purpose of information disclosure, see Eungkyoon Lee, 'Information disclosure and environmental regulation: Green lights and grey areas' (2010) 4(3) Regulation & Governance Journal 303, Page 316.

[661] "Regulatory agencies will be able to speak more softly when they are perceived as carrying big sticks." (See, Ayers and Braithwaite (n 637), Pages 5-6). This highlights that regulators must have a variety of sanctions available to them. By showing a willingness to escalate to a higher sanction, theoretically society will be more compliant. Society is more likely to accept regulation if there is the possible threat of a tougher sanction. This could be because the regulator is perceived as fair where they do not use the most intrusive form of regulation. This further enhances the potential benefits of adopting the decentred perspective of regulation which encompasses more 'regulatory options' than the traditional approach.

5.2.2: Julia Black's Approach of Decentred Regulation

Decentred regulation can be described as the polar-opposite view to the "central meaning" of regulation in the previous section.[662] Black's idea of decentred regulation acknowledges the multi-disciplinary approach that can be regarded as a necessity for socially informed regulation in the modern era.[663] Similar to Morgan & Yeung, Julia Black acknowledges the assumption of state involvement but suggests that regulation must be regarded as a more intricate idea.[664] Removal of the necessity of state involvement achieves a more accurate representation of regulation in modern society.[665] Such an approach may be especially appropriate when considering the unique legal issues posed by unpermissioned blockchain technology.[666]

Decentred regulation is defined as "the sustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour-modification."[667] Regulation under a decentred perspective can be seen as "an intentional, systematic attempt at problem-solving, so marking it out as a specific site of social activity and thus of investigation".[668] It is a broader view of regulation, whereby even self-regulation may be viewed as a form of regulation.[669]

---

[662] Black (n 622), Pages 3-8.
[663] Daniela Aguilar Abaunza, *The Law for Energy Prosumers* (Springer 2022), Page 85; Black (n 622), Page 6. Claus Offe would suggest that interdependencies create the need for co-produced regulation by society and the government, utilising the capacities of both, to solve the needs of both where possible. See Claus Offe, *Contradictions of the Welfare State* (Routledge 1984), Page 310.
[664] Black (n 622), Page 2; Shuchi Bharti, *Corporate Social Responsibility in India* (Palgrave Macmillan 2022), Pages 29-36. This is due in part to globalisation and changes in societal understanding.
[665] Daniela Aguilar Abaunza, *The Law for Energy Prosumers* (Springer 2022), Page 91.
[666] For a discussion of how decentred regulation provides a more community-based approach with various stakeholders potentially being involved and how this may apply in the context of corporate social responsibility see, Shuchi Bharti, *Corporate Social Responsibility in India* (Palgrave Macmillan 2022), Pages 29-36.
[667] Black (n 622), Page 26.
[668] Ibid.
[669] For some additional possible definitions and some of their issues, see Baldwin, Cave and Lodge (n 62), Page 3; Black (n 622), Page 11.

Regulators must seek solutions for regulating unpermissioned blockchain technology and must recognise that the law itself will not alter the technology or its desirability. The technology exists and can disrupt the traditional models in many sectors.[670] As noted, the options for "regulation" are broader under Julia Black's "decentred regulation" theory.[671] Black recognises the complexity of society and that there are many ways in which behaviour can be altered, which therefore increases the potential "regulation" to include more than mere black letter law.[672] Potential policy choices will be explored following the discussion of whether regulation of unpermissioned blockchain technology for systematic errors would be deemed justifiable and necessary.

5.3: Is regulation for fault within unpermissioned blockchain technology justifiable?

Motives for regulation and justifications for regulation are distinct from one another.[673] Motivations can be influenced by stakeholders and reasons such as an upcoming election.[674] Depending on one's view of regulation it may be seen as a "green light concept" with a perception that markets will sometimes, inevitably require regulation to reach maximum efficiency (as it creates and protects rights).[675] Alternatively, anti-regulationists view regulation as a "red light concept" as it prohibits or prevents the normal balance of conduct (efficiency)[676] that would be brought about in a free market system.[677] This notion of the perfect market ("heavenly markets theory")

[670] UK Government Chief Scientific Adviser (n 237), Page 14.
[671] Walter Johnson, 'Flexible regulation for dynamic products? The case of applying principles-based regulation to medical products using artificial intelligence' (2022) 14(2) Law Innovation and Technology 205, Page 216; Black (n 622), Pages 3 and 4.
[672] Julia Black, 'Constitutionalising Regulatory Governance Systems' (2021) LSE Law, Society and Economy Working Papers 02/2021 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3813812> Accessed 1st February 2023, Page 6; Black (n 622), Page 26.
[673] Baldwin, Cave and Lodge (n 62), Page 15.
[674] Ibid.
[675] Ibid, Page 3.
[676] Ibid. This can fall into the idea of private interest theory of regulation. For more discussion on this see, Morgan and Yeung (n 649), Page 44.
[677] Baldwin, Cave and Lodge (n 62), Page 3.

which will always produce the most efficient outcome is impractical. Therefore, regulation of unpermissioned blockchain technology has the potential to create rights for end users, but it may restrict personal choice. Consequently, use of regulation for unpermissioned blockchain technology must be scrutinised or else risk infringement of personal choice, stifled usage of the technology[678] or excessive bureaucracy.[679]

This section shall proceed by examining the justification of correcting a market failure[680] and applying this to unpermissioned blockchains. This approach requires examination of the main economic justification for regulation. If this can be applied to unpermissioned blockchain technology it would suggest a potential transition from the "market system" of leaving the market to regulate itself, to the "collectivist system" whereby regulation is viewed as essential to correct a market that fails.[681] Following on from this, the most novel and potentially applicable to unpermissioned blockchain technology is Julia Black's theory that risk is a justification for regulation.[682]

5.3.1: Correcting market failure

Viewing regulation through an economic lens is common.[683] This results in a focus on markets and how regulation can impact them. To understand why correcting a market failure is a justification for regulation, some key economic principles need to be

[678] For an example of some countries to 'ban' Bitcoin see, cryptonews.com (n 246). 'Ban' is used in quite liberally, as some countries have an 'indirect ban' where trading Bitcoin is extremely difficult and inaccessible, but there is no explicit or direct ban.
[679] Control of societal behaviour is not an easy feat. It can result in problems such as societal non-compliance or over-restriction from the law which prevents social change. See Regine Paul and others (eds), *Society, Regulation and Governance: New Modes of Shaping Social Change?* (Edward Elgar Publishing 2017), Page 5. For a discussion on the risk of overly 'bureaucratic' law, see Shleifer (n 625), Page 439.
[680] Monopolies and wastage will be assessed in the context of unpermissioned blockchain technology. A detailed analysis of every potential sub-justification is not necessary for the purpose of this thesis as some forms of market failure are not as applicable to unpermissioned blockchain technology. See section 5.3.1.
[681] Anthony Ogus, *Regulation: Legal Form and Economic Theory* (Clarendon Press 1994), Chapters 2-3.
[682] See section 5.3.2; Black (n 151).
[683] See the discussions in section 5.4 relating to the market theory; Ogus (n 681), Chapter 2.

discussed.[684] From an economic understanding, everything can be analysed as a market.[685] When assessing the market, in theory there is an efficient point of operation. This is known as "economies of scale" and is where the supply and demand of a market is met.[686] It is only if we consider the market as an imperfect system that regulation can be assessed as a viable solution should the market fail.[687]

The traditional example of a market failure[688] is a monopoly that has significant control over the market. [689] In such a scenario, regulation could be used to cap the pricing, to protect the final consumer.[690] However, due to the decentralised nature of the technology that underlies many cryptocurrencies, it would be difficult to apply the concept of monopoly power to unpermissioned blockchain technology. Therefore, this section will explore an alternative form of market failure applicable to unpermissioned blockchain technology.

---

[684] Justifying regulation because of a market failure is largely based on two assumptions: that markets are prone to failure and the regulation is costless (and potentially necessary). See Michael Hantke-Domas, 'The Public Interest Theory of Regulation: Non-Existence or Misinterpretation?' (2003) 15 European Journal of Law and Economics 165, Page 165; Shleifer (n 625), Page 440.

[685] Even society can be perceived through the idea of 'markets'. Whilst the dictionary definition of 'market often refers to buying and selling of goods and services, it can also reference an industry or a group of people. See Cambridge Dictionary, 'Market' (2021) <https://dictionary.cambridge.org/dictionary/english/market> Accessed 1st February 2023 for various definitions.

[686] Theoretically the common idea of market efficiency is whereby the 'consumer' has choice and can pick based on the own autonomous preferences.

[687] It may be said that those who believe regulation is the only solution to market failures may be susceptible to the 'nirvana fallacy'. The 'nirvana fallacy' is where there is a belief that there is a perfect solution to a particular problem. One solution may not be the only capable solution to a problem, and no single solution may fully resolve an issue. There is no perfect outcome as a market is not perfect nor is regulation perfect. This can be regarded as a similar concept to the 'heavenly markets theory' raised in section 5.3. Consequently, for the lack of legal redress of systematic errors within unpermissioned blockchain technology there is no perfect solution. Any proposed solution will need to find the balance of protecting risk in a fast-moving technology without stifling enterprise. To attempt to mitigate the 'nirvana fallacy', one possibility could be conducting a cost-benefit analysis. For more discussion on this see, Michael Hantke-Domas, 'The Public Interest Theory of Regulation: Non-Existence or Misinterpretation?' (2003) 15 European Journal of Law and Economics 165, Page 188.

[688] It is also worth noting that under the free market ideology, monopolies have the potential to be considered as efficient. For more discussion on efficient monopolies see, Baldwin, Cave and Lodge (n 62), Pages 16-17; Morgan and Yeung (n 649), Page 18.

[689] Baldwin, Cave and Lodge (n 62), Page 16. For further discussion into why control and not market share should be the key determinant of monopoly power see, Shirin Ghaffary and Jason Del Rey, 'The Big Tech antitrust report has one big conclusion: Amazon, Apple, Facebook and Google are anti-competitive' (2020) <https://www.vox.com/recode/2020/10/6/21505027/congress-big-tech-antitrust-report-facebook-google-amazon-apple-mark-zuckerberg-jeff-bezos-tim-cook> Accessed 1st February 2023.

[690] Baldwin, Cave and Lodge (n 62), Page 16.

The main form of market failure that could be suggested in the cryptocurrency and unpermissioned blockchain technology markets would be wastage. Where the proof-of-work validation method is relied upon, such as in Bitcoin, there is a significant damage to the environment.[691] It is worth noting that the proof-of-stake validation method does result in a much lower amount of energy consumption,[692] however, the present wastage may increase if further interaction in these cryptocurrency markets continues. The Government Office for Science acknowledge this potential for societal "knock-on effects"[693] if further use of decentralised platforms such as those which utilise unpermissioned blockchain technology.[694] Prosser's justification of regulation for the purpose of social solidarity and citizenship can also be relevant here.[695] Prosser gives the example that regulation of the environment can further social objectives and encourages togetherness. In Prosser's view of regulation these outcomes can be achieved even if there is not a market failure that can be clearly defined.[696] The environmental impact here of unpermissioned blockchain technology is more akin to wastage as a market failure than regulation to protect the environment through social solidarity due to the current level of usage. However, the potential for justification remains. Consequently, regulation may be justified due to the potential harm to the environment and the knock-on effects of the technology.[697] Although it is relevant to note that environmental impacts may ultimately be addressed through the market gravitating towards proof-of-stake and so may not justify regulation presently.

---

[691] Baraniuk (n 315); Liana Badea and Mariana Claudia Mungiu-Pupazan, 'The Economic and Environmental Impact of Bitcoin' (2021) 9 IEEE 48091; Alex de Vries, 'Bitcoin boom: What rising prices mean for the network's energy consumption' (2021) 5(3) Joule 509; Anh Ngoc Quang Huynh and others, 'Energy Consumption and Bitcoin Market' (2022) 29 Asia Pacific Financial Markets 79.
[692] For more information on proof-of-stake see, Hari and Pasquier (n 184), Page 427.
[693] Government Office for Science (n 8), Page 44.
[694] Ibid.
[695] Tony Prosser, 'Regulation and Social Solidarity' (2006) 33(3) Journal of Law and Society 364, Page 364.
[696] Baldwin, Cave and Lodge (n 62), Page 22.
[697] Ibid, Page 18. It may be difficult to determine whether the scope and extent of the regulation is justified. This is because the speculative nature of potential harm to future generations is tough to comprehend. See Morgan and Yeung (n 649), Page 22.

5.3.2: Risk as a justification

Potential justifications for regulation are broad and a range of rationales can apply in cohesion with one another.[698] As a result, regulation is capable of being extended into various aspects of society providing one justification is applicable.[699] Arguably the most compelling justification of regulation is the theory that sufficient risk may be a reason to regulate.[700] The idea of risk being a justification for regulation seems promising for unpermissioned blockchain technology due to the high levels of risk associated with the technology.[701]

The meaning of "risk" for the purpose of this thesis has previously been discussed,[702] the risk of errors or faults that can impact the value of the asset stored on the unpermissioned blockchain in line with Renn's definition of risk whereby human actions may have consequences on aspects we value.[703] Black notes that advancements in technology can create new risks or alter the types of risks within society.[704] In the risk-approach to regulation, Black specifies that the "government's role is to manage risk, and it is justified in intervening in society in the pursuit of that objective."[705] In stating this, Black is pointing out that regulation is one of the tools to manage risk. This

[698] Baldwin, Cave and Lodge (n 62), Page 23.
[699] The justification of regulation and its scope are two distinct features. Regulation may be justified for a particular issue. The scope of the subsequent regulation will be subject to further scrutiny.
[700] Black (n 151), Page 304.
[701] See the variety of 'risks' within Chapter 2, specifically section 2.5 and 2.6. It could also be mentioned that under the private interest theory of regulation, there is the concept that individuals will demand regulation when they require it. See, Morgan and Yeung (n 649), Page 43. This is important within the context of unpermissioned blockchain technology and DLT more generally. As previously stated, the concept of market failure is difficult to align with this decentralised technology. Instead, it is more likely that regulation will be developed in a reactionary manner when more individuals engage with the technology. This may also explain why currently there is a lack of legal redress. However, as usage of the technology increases, the demand for regulation will potentially increase. For more discussion on private interest theory, see David Haddock and Jonathan Macey, 'Regulation on Demand: A Private Interest Model, with an Application to Insider Trading Regulation.' (1987) 30 Journal of Law and Economics 311, Page 312.
[702] See the discussion of risk in section 2.1.1. Black acknowledges that there are a variety of 'risks' in modern society, referring to the notion of sociology that we live in a 'risk society'. This means that society must manage the risks that society itself has created. See, Black (n 151), Page 302.
[703] Renn (n 165), Page 51.
[704] For an interesting discussion on how society's view of risk can be impacted, see Black (n 151), Pages 313-314.
[705] Ibid, Page 306.

ties in with the novelty of unpermissioned blockchain technology and how its interaction with the law may require a unique approach.[706]

As referenced previously, some forms of risk must be managed by the individual themselves; the concept of risk is a part of life.[707] The continuous use of regulation to minimise risk is a paternalistic approach.[708] There is the potential to over-protect society from more trivial risks which would result in a "nanny-state". This reflects the FCA's present approach regarding cryptocurrency investment, whereby they do not prohibit investing, but warn of the risks associated.[709] Therefore, there must be a consideration of whether a consensus exists for a risk being important enough to justify regulation.[710] A subjective view of risk would provide no benefit to the potential justification of regulation.[711] The question therefore becomes whether the lack of legal redress for systematic errors within unpermissioned blockchain technology is a risk that is objectively justifiable to "regulate". This links with the idea previously that regulation is not the appropriate solution for every societal, economic or legal issue and a balanced approach must be sought.[712]

Black considers the necessity of stabilising the decision-making of risk-based regulation.[713] One potential method is the "precautionary principle" which is a purely

[706] This theme has been present throughout this thesis.
[707] Black highlights the fine balancing act between paternalism and over-protecting society in the form of a 'nanny-state'. See, Black (n 151), Pages 306-307.
[708] Ibid, Page 304.
[709] Financial Conduct Authority (n 569).
[710] Black (n 151), Page 311.
[711] Ibid. See the discussion of how risk can alter dependent on various factors.
[712] The balancing act is further complicated when considering the trade-offs of risk-based regulation. Within unpermissioned blockchain technology regulation will not satisfy the interests of every participant. For example, anti-money laundering regulations within this field may be for the benefit of the general public as it seeks to stifle the criminal usage of cryptocurrency and limit the funding of terrorism. However, for those criminals and other parties wishing to operate outside of the regulatory sphere it would certainly not appease them. For further discussion of potential trade-offs when concerning with risk-based regulation and the difficulty to quantify risk statistically see, Black (n 151), Pages 309, 310 and 316. For discussion of the desire of the UK government to provide a balanced and proportionate approach to regulation in this field see, HM Treasury (n 120), Pages 35, 57 and 68.
[713] Black (n 151), Pages 312 and 317.

political method of decision-making.[714] This can provide a degree of flexibility but also creates a justification to regulation which is viewed as fuelling political motives.[715] An alternative method involves asking the question of when something is too risky. This is known as a cost-benefit analysis.[716] However, this too has its downfalls as there can be issues determining the true costs involved for all parties[717] and this is likely to be applicable in a volatile market such as cryptocurrency,[718] which has been the predominant use for unpermissioned blockchain technology thus far.

Risk, consequently, can provide a potential justification for regulation but is somewhat problematic in application in the context of unpermissioned blockchains. Some of these issues can be resolved through methods such as the "precautionary principle" or a cost-benefit analysis,[719] to stabilise the decision-making of when to regulate risk. However, these methods are not perfect. The nature of regulation itself can result in uncertainty and complexity.[720] Black provides a possibility for regulation to be justified within unpermissioned blockchain technology due to the presence of risk. The main stumbling block is providing a consistent method to analyse the severity of risk. Nevertheless, risk may provide the most suitable justification for regulation in the context of unpermissioned blockchain technology. The control of risk has therefore been selected as a justification for decentred regulation and will now be applied in the consideration of how Chiu's four approaches can be used to address risk in crypto.

[714] Some are suspicious that it is a clever ploy from politicians to justify certain political approaches. Nonetheless it has still developed to be a key "principle of risk regulation in the EU." There has been a gradual acceptance of this principle within the UK also. See, Black (n 151), Pages 318, 319 and 321.
[715] Oliver James, 'Regulation Inside Government: Public Interest Justifications and Regulatory Failures' (2002) 78(2) Public Administration 327, Pages 334-339.
[716] Black (n 151), Page 321.
[717] Ibid, Page 322.
[718] Financial Conduct Authority (n 113), Page 9.
[719] Black (n 151), Page 322.
[720] James (n 715), Page 335.

5.4: Policy choices

As the UK government have expressed a desire for a flexible approach to regulation within this field as usage rises,[721] the approach of Black potentially offers this. As a context specific discussion of regulatory choices, this section will however primarily be framed around Chiu's four policy choices,[722] which identify approaches of different levels of intervention. There are a range of potential policy choices available if regulators wish to further protect investors and some will be explored now, evaluating present UK approaches and policies based around Chiu's framework.

5.4.1: Ensuring users can manage their own risk

Chiu suggests that four potential policy choices could be taken for cryptocurrency regulation with the first policy choice being "to ensure that those engaged in it are able to manage the risks of their activity".[723] This approach reflects the present UK approach of alerting consumers to the risks present and trying to increase the awareness of those risks so the consumers can then manage them.[724] However, in seeking to alert consumers of risk there is also a desire to not interfere too much in the market itself, [725] which can be described as the free-market view of regulation. The free-market approach empowers the market by granting power and protecting rights of the market.[726] The logic here is that due to the nature of the market itself, the market is best placed to regulate itself and achieve efficiency.[727] As will be discussed below, unpermissioned blockchains might be left for self-regulation under this approach and, given this likelihood, an approach based on Ostrom's work will be considered below.

[721] HM Treasury (n 120), Pages 8-11.
[722] Chiu (n 100), Page 263.
[723] Ibid.
[724] Ibid, Page 264.
[725] HM Treasury (n 120), Pages 5, 7, 10-11, 57, 67-68 and 77.
[726] Ogus (n 681), Chapter 2; Prosser (n 651), Page 7.
[727] This emphasis on the freedom of the market, the freedom of society and the freedom of individuals is synonymous with a libertarian view of regulation. Ogus (n 681), Chapter 2.

A danger is that the response is reactive rather than proactive.[728] This could suggest a reason why the vulnerability of consumers to these cryptocurrency scams seems to be increasing, as the current consultation indicates.[729] The FCA has however acknowledged that "Consumers may buy cryptoassets without being aware of the limited regulatory protections".[730]

Consumer protection presents a more compelling case for greater regulation than prescription about activities of financial institutions. "Regulators are unlikely to make prescription in terms of 'what not to do' in relation to speculative financial activity engaged by financial institutions. Regulatory governance is crafted more along the lines of imposing duties on financial institutions to risk manage prudently".[731] It is possible to view a licensing system imposed on the exchanges as an imposition of a duty to manage the risk prudently through regular security updates or checks, which is discussed below. However, Chiu suggests here that a list of trusted cryptocurrencies may be unlikely to be provided by regulators in the UK as it would imply what not to do. This appears to be in line with the recent consultation paper whereby the UK government acknowledge that a balance must be struck between regulating and the threat of over-regulation which can stifle innovation.[732]

5.4.2: Incentivising good governance

The second policy choice would be to discourage poorly governed unpermissioned blockchain technology cryptocurrencies through "incentive-based regulation".[733] This is where the regulated firm, is encouraged through rules to reach the

[728] Chiu (n 100), Page 264.
[729] HM Treasury (n 120), Pages 5 and 9.
[730] Financial Conduct Authority (n 113), Page 12.
[731] Chiu (n 100), Page 264.
[732] HM Treasury (n 120), Page 5. For further discussion of the potential impact of regulation on innovation see, Knut Blind, 'The Impact of Regulation on Innovation' in Jakob Edler and others (eds), *Handbook of Innovation Policy Impact* (Elgar Publishing 2016), Pages 450-482.
[733] Chiu (n 100), Page 263.

desired goal with some, although not full discretion afforded to the firm.[734] Although *permissioned* blockchain platforms are not free of issues, it could be beneficial if governments encouraged and incentivised the use of permissioned blockchain technology, which conforms to the traditional legal system more easily. The same considerations would apply to encouraging well-run unpermissioned blockchains. Such a policy choice would not necessarily prevent the potential for cryptoasset scams and poor maintenance standards in unpermissioned blockchain platforms nor would it prevent the use of and investment in cryptocurrencies based on unpermissioned blockchains.[735]

The anonymity of those involved in unpermissioned blockchain technology means that even an outright ban on the platforms would be difficult to enforce. Individuals may merely engage in "regulatory arbitrage" to place themselves in more favourable legal circumstances.[736] In turn, this can leave customers within those markets as under-protected and potentially exposed to greater risks of scams, hacks, or volatility. Theoretically a licensing system could be implemented in relation to cryptocurrency markets specifically, as considered in the next section, but this would not provide protection for any issues occurring on the underlying blockchain.

5.4.3: Controlling risk through pre-vetting and licensing

The third policy choice would be where cryptocurrencies are "subject to pre-vetting and approval."[737] As stated previously, this could involve a list of trusted cryptocurrencies, which may include stablecoins[738] and central bank digital

[734] Per Joakim Agrell, 'Incentive Regulation of Networks: Concepts, definitions and models' (2015) 1(2) Reflets et Perspectives de la vie Economique 103, Page 107.
[735] Chiu (n 100), Page 265.
[736] Victor Fleischer, 'Regulatory Arbitrage' (2010) 89 Tex L Rev 227, Page 229.
[737] Chiu (n 100), Page 264.
[738] For a detailed discussion on stablecoins see, Dirk Bullman, Jonas Klemm and Andrea Pinna, 'In search for stability in crypto-assets: are stablecoins the solution?' (August 2019) No 230 European Central Bank Occasional Paper Series <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3444847> Accessed 1st February 2023.

currencies[739] for example but would involve a significant change in policy from the current regulatory approach in the UK. There are compelling arguments that such a paternalistic approach of pre-vetting could be warranted to manage the risk that is present in cryptocurrencies and a variety of regulatory techniques could fall into the pre-vetting concept.[740] "Regulators could demand that developers include code that builds in safeguards against systematic stability risks."[741] This could reduce the threat of systematic errors such as hacking which could result in a more protected exchange customer. Although some cryptocurrencies, in particular stablecoins, have attempted to project a veneer of trustworthiness and security it is worth mentioning that even stablecoins are not necessarily without risk.[742]

A problem with a pre-vetting approach is that it could stifle innovation and lead to embedding of weaker crypto options within the market.[743] It is also unclear what the impact would be of such a pre-vetting regulatory approach. There is the possibility that consumers would be drawn towards these regulated and trusted cryptocurrencies and such cryptocurrencies could increase in value.[744] However, it is also possible that part of the appeal of these decentralised cryptocurrencies such as Bitcoin is the perceived lack of governmental control. It seems from past events that regulatory indication of acceptance can result in increased value of the cryptocurrency and vice versa. When Japan indicated that Bitcoin would be considered legal tender, the price of Bitcoin

[739] For a discussion on how central bank digital currencies could impact economic policies see, Michael Bordo and Andrew Levin, 'Central Bank Digital Currency and the Future of Monetary Policy' (August 2017) Working Paper 23711 NBER Working Paper Series <https://www.nber.org/system/files/working_papers/w23711/w23711.pdf> Accessed 1st February 2023.
[740] Chiu (n 100), Page 266; See also the discussion in HJ Allen, 'Driverless Finance' (2020) 10 Harvard Business Law Review 157.
[741] Chiu (n 100), Page 266.
[742] For a discussion into the 'stability' of 'stablecoins' see, Usman Chohan, 'Are Stable Coins Stable' (29th March 2020) Notes on the 21st Century (CBRi) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326823> Accessed 1st February 2023.
[743] For further discussion on the threats of such a paternalistic approach see, Stacey Dogan and Mark Lemley, 'Antitrust Law and Regulatory Gaming' (2009) 87 Texas Law Review 685.
[744] For a brief discussion into some positives that regulation could bring the cryptocurrency market see, (sygna.io), 'Why Regulations Will Benefit the Crypto Industry in the Long Run' (2020) <https://www.sygna.io/blog/why-regulations-will-benefit-the-crypto-industry-in-the-long-run/> Accessed 1st February 2023.

rose.[745] Conversely, when China sought to effectively ban Bitcoin trading, the price plummeted.[746] Either of these policies would be a stark contrast to the current regulatory approach in the UK. The likelihood of UK regulators changing their current policy imminently is therefore limited, although in the latest consultation paper there is the recognition for the need to be flexible as the technology and consumers interaction with it evolves.[747] Therefore, if regulators wish to draw more of the cryptocurrency market towards permissioned blockchain cryptocurrencies, which may be more easily regulated due to the presence of a central party and the lack of anonymity, or at least encourage better internal governance standards of unpermissioned blockchains, then a policy change may be a necessary aspect to consider.

Presently there has been little done to signal preferences for any type of cryptocurrency, with more general public protection measures in response to particular harms. Investors into crypto are presently afforded some protection through advertising controls and there is an expectation that they manage their own risks.[748] There is presently the requirement of registration for anti-money laundering purposes,[749] which represents a public protection measure, although there is the prospect of a considerable tightening of regulation in this area.[750] Registration is necessary for all firms that engage in cryptoasset and such registration or licensing system could be extended to increase its scope of concern.[751]

[745] Alicia Cameron and Kelly Trinh (theconversation.com), 'Four factors driving the price of Bitcoin' (November 2017) <https://theconversation.com/four-factors-driving-the-price-of-bitcoin-87244> Accessed 1st February 2023, See 'Regulatory moves'.
[746] Ibid.
[747] HM Treasury (n 120), Pages 10-11.
[748] Financial Conduct Authority (n 113), Pages 11-13.
[749] Financial Conduct Authority, 'Register Cryptoasset firms' <https://register.fca.org.uk/s/search?predefined=CA> Accessed 1st February 2023.
[750] HM Treasury (n 120), Pages 10-11.
[751] For more information on such a registration requirement, see Financial Conduct Authority (n 511); Financial Conduct Authority, 'Do I need to register with the FCA for carrying on cryptoasset activity?' (2019) <https://www.fca.org.uk/publication/documents/cryptoasset-registration-flowchart.pdf> Accessed 1st February 2023.

A further possibility would be a licensing requirement for exchanges. The present registration requirement could be extended into a licensing system as an attempt to mitigate some of the threats of hacking and scams present in the exchange and DEX methods. Examples of scams include the Squid Game cryptocurrency scandal, whereby creators made allegedly almost 2.5 million pounds,[752] or the infamous "OneCoin" scandal which saw investors across the world pour approximately 2 billion pounds into this fraudulent cryptocurrency.[753] In America, it has been estimated that between the 1st October 2020 and the 31st March 2021 over 50 million dollars was stolen in over 6500 cryptocurrency scams.[754] The vulnerability of consumers and presence of scams in the cryptocurrency market suggest a threat of public harm beyond that of money laundering that could warrant regulatory intervention.[755] Therefore the lack of redress for faults in the blockchain is part of a wider set of risks that might lead to greater regulation.

The UK has shown a willingness to adopt such a licensing system in the gambling sector for example,[756] which bears some similarities to cryptocurrency investment due to the volatility present.[757] If a licensing system were developed, exchanges could be expected to impose requirements for crypto coins they list, akin to the Listing Rules for shares which protect investors through disclosure and other measures.[758] A heighted prudential requirement could mitigate some of the bad

[752] (bbc.co.uk), 'Squid Game crypto token collapses in apparent scam' (November 2021) <https://www.bbc.co.uk/news/business-59129466> Accessed 1st February 2023.
[753] Jamie Bartlett (bbc.co.uk), 'Missing Cryptoqueen: Why did the FCA drop its warning about the OneCoin scam?' (August 2020) <https://www.bbc.co.uk/news/technology-53721017> Accessed 1st February 2023.
[754] Emma Fletcher (ftc.gov), 'Cryptocurrency buzz drives record investment scam losses' (May 2021) <https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses> Accessed 1st February 2023.
[755] Black (n 151), Pages 303-304. This potential 'risk' that could justify regulatory intervention will be discussed further in the following chapter. See section 5.3.2.
[756] Gambling Act 2005. For further information see, Gambling Commission, 'Home' <https://www.gamblingcommission.gov.uk/> Accessed 1st February 2023.
[757] Paul Delfrabbro and others, 'Cryptocurrency trading, gambling and problem gambling' (2021) 122 Addictive Behaviours 1, Pages 1-2; Financial Conduct Authority (n 113), Page 9.
[758] Section 73A Financial Services and Markets Act 2000 grants the FCA right to alter and update such listing rules which can be found here, Financial Conduct Authority, 'The Listing Rules' (January 2023) <https://www.handbook.fca.org.uk/handbook/LR.pdf> Accessed 1st February 2023.

corporate governance standards which can be adopted without closer regulation as indicated with an example such as FTX.[759] However, it would provide no benefit to the threat of malicious nodes or forks within the underlying blockchain technology.

Two key focuses would be present in such a licensing system; firstly, enhanced security of the exchanges themselves, potentially achieved by regular coding checks or updated security practices based on industry standards. The second and arguably most important focus would be the requirement for segregation and safe keeping of client money.[760] This would provide increased protection and practicality should any errors occur, as in theory it will be easier to identify client property and potentially return such property in the event of errors or bankruptcy.

In the recent consultation paper on cryptoasset regulation, the UK government have acknowledged that segregation of client assets could be an important component for consumer protection in this field.[761] Segregation is also a requirement that the US Securities and Exchange Commission (SEC) has indicated that they will begin looking at to regulate the conduct of cryptocurrency exchanges.[762] In doing so, Gary Gensler, the chair of the SEC, points to statistics which suggest that fourteen billion dollars' worth of crypto-assets were stolen in 2021 and such a segregation of assets could be a necessary step.[763] Gensler also highlights that the function of cryptocurrency exchanges is similar to traditional exchanges.[764]

This recommendation of exchange licensing is not without risk. There is the possibility that a licensing system would be viewed within the industry as over-

[759] Calhoun (n 548).
[760] This has been a significant issue in relation to exchanges that have failed, such as QuadrigaCX. For more information see, Tim Copeland (decrypt.co), 'The complete story of the QuadrigaCX $190 million scandal' (March 2019) <https://decrypt.co/5853/complete-story-quadrigacx-190-million> Accessed 1st February 2023.
[761] HM Treasury (n 120), Page 52.
[762] Gary Gensler, 'Prepared Remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference' (April 2022) <https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422> Accessed 1st February 2023.
[763] Ibid.
[764] Ibid.

burdensome. In such event, it could prompt regulatory arbitrage, similar to the catastrophic New York licensing attempt which resulted in exchanges moving out of the State and continuing operations without any change in practice.[765] This was largely due to the length of the application for obtaining a license and the ease for such exchanges to simply move to the next State.[766] The risk here from the perspective of England is that the market will be seriously affected if exchanges decide to move out of country to avoid such a system. There is the acknowledgement from the UK government that exchanges can operate outside of the jurisdiction if they wish to avoid such rules, however in such an event the regulatory focus would then become mitigating the threat of UK customers still accessing those exchanges as enforcement on the exchanges can become more difficult.[767]

Regarding the current requirement for firms who engage with cryptoassets to register, some industry insiders have been seemingly left frustrated as figures suggest that "80% of the firms… have either withdrawn their applications or been rejected."[768] Reasons for this could be credited to the slow processing times of the application. This could suggest that parallels may be drawn between the FCA's requirement of registration and New York's licensing system.[769] It would therefore be essential that alongside the recommendation of a licensing system for exchanges, there is a streamlined process in place. Although there is also the possibility that the current lack

[765] For some discussion of this, see Daniel Roberts (fortune.com), 'Behind the "exodus" of bitcoin startups from New York' (August 2015) <https://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/> Accessed 1st February 2023.
[766] Banking on Bitcoin Documentary (n 206).
[767] HM Treasury (n 120), Pages 57-58.
[768] Ryan Browne (cnbc.com), 'A total disaster: Crypto firms face being booted from the UK as a key deadline approaches' (March 2022) <https://www.cnbc.com/2022/03/24/crypto-firms-face-being-booted-from-uk-as-fca-register-deadline-nears.html> Accessed 1st February 2023.
[769] For an interesting discussion on how the UK, US and EU are trying to regulate exchanges see, Matthew Elderfield, 'How to supervise a crypto exchange' (December 2022) <https://www.ft.com/content/6e2bd1b3-aa4a-40a2-9788-05ced5c1e0fc> Accessed 1st February 2023.

of registrations may be viewed positively as potentially poorly run exchanges may be taken off the market.[770]

Furthermore, the FCA would also benefit from learning from the mistakes of the Financial Services Agency (FSA) in Japan.

> *"In 2017, Japan passed laws requiring cryptocurrency exchanges to register with the Financial Services Agency (FSA). Yet when a theft occurred from exchange Coincheck in 2018, the FSA could do little more than recommend… the firm improve its security processes because it did not have any rules in place allowing it to deal with the type of attack used by the thieves."*[771]

Any attempts to further protect exchange-customers from the risks of trading through exchanges would need to have a smooth and efficient registration system and have a clear structure in place for how to effectively deal with any harm that arises. This discussion of a potential licensing system indicates that alternatives to the current approach exist, but they may not resolve the issue entirely.

5.4.4: Allocative financial regulation

The fourth and final policy choice is completely paternalistic as it is a restriction on market freedom through "allocative financial regulation"[772]. This is where regulation is used to shift the allocation of financial capital away from more speculative activities.[773] For example, if permissioned cryptocurrencies or centralised digital currencies were supported in the public sector, this could steer investment towards these means and away from the volatile unpermissioned cryptocurrency market. This would

[770] For a list of unregistered cryptoasset firms in the UK see, Financial Conduct Authority, 'Unregistered Cryptoasset Businesses' (February 2022) <https://register.fca.org.uk/s/search?predefined=U> Accessed 1st February 2023.
[771] Howell and Potgieter (n 131), Page 5.
[772] Chiu (n 100), Page 271.
[773] Ibid, Page 270.

involve a complete and institutionalised policy shift and is one that may be considered for overall economic development.[774]

There is some potential of the UK beginning to move in this direction with discussion of a digital currency backed by fiat currency being introduced by the Bank of England by approximately 2030.[775] Although this is a possibility within the next decade, the UK government also state that it is currently too soon to create a centrally backed digital currency, merely that it is the next logical step.[776] Thus meaning it is probable but only when the market necessitates its formation.[777] This may also be seen as part of the regulatory roadmap whereby in the recent consultation, the flexible approach states that further involvement in the market will arise should market integrity or macroeconomic instability be impacted.[778] As usage in the crypto market increases, one regulatory choice can be to steer the consumers to this centrally backed digital currency as an alternative to the instable cryptocurrencies presently, which can have greater risks of economic instability where usage increases.[779] Therefore, although it is a potential policy choice available, it would seemingly only manifest when the market determines it necessary.[780] Such an approach could also be negatively received in the cryptocurrency market as it appears to be in opposition "to the [potential anti-establishment] ethos in the crypto-economy".[781] This can show the careful balance between regulation and stifling innovation or the free market principle.

It is clear therefore that alternative policies exist to the current regulatory approach and with the UK government having recently indicated the need for an

[774] T Lothian, *Law and the Wealth of Nations* (New York: Columbia University Press 2016), Chapter 2.
[775] HM Treasury, 'The digital Pound: a new form of money for households and businesses?' (CP797, February 2023) <https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper> Accessed 7th February 2023, Pages 7-12.
[776] Ibid, Page 7.
[777] Ibid.
[778] HM Treasury (n 120), Pages 8-11.
[779] Ibid, Pages 10-11.
[780] HM Treasury (n 775), Page 7; HM Treasury (n 120), Pages 8-11.
[781] Chiu (n 100), Page 271.

evolving approach to regulation in this field,[782] the potential for a change in policy is enhanced. Other policy choices could result in further protection for exchange customers but would be unlikely to increase protection for peer-to-peer users in respect of systematic errors within unpermissioned blockchain technology.

There is the capability to use regulation as a method to divert the use of cryptocurrencies away from the decentralised cryptocurrencies and towards permissioned blockchain cryptocurrencies, stablecoins with proper asset backing or centralised digital currencies backed by fiat currency.[783] In theory, as permissioned blockchain is centrally controlled, it is more compatible with a fault-based liability system. Therefore, if customers switched from cryptocurrency that utilises unpermissioned blockchain technology to cryptocurrency which relies on permissioned blockchain technology, then the ease of applying the current framework of law in respect for legal redress would be enhanced. This is largely due to the identities of parties being known and the centralisation of such platforms which can provide a potential defendant and a party for legal obligations/restrictions to be attached to. However, it is important to recognise that such a policy choice wouldn't necessarily prevent the popularity of the decentralised cryptocurrencies and may merely result in "regulatory arbitrage". Consequently, whilst increased regulatory protections could be afforded to exchange customers, it can only arise from a regulatory desire to do so as it involves a policy change from the current regulatory approach.[784] Furthermore, if increased regulatory protection of peer-to-peer users or DEX customers is desired, a more creative policy choice that "more robustly interacts with the features of"[785]

[782] HM Treasury (n 120), Pages 10-11.
[783] Stablecoins have been mentioned in the latest consultation as an area that the proposed Financial Services and Markets Bill will bring in a regime to regulate. For further discussion see, HM Treasury (n 120), Pages 11-12 and 16; Financial Services and Markets Bill, (HL Bill 80) <https://bills.parliament.uk/publications/49063/documents/2625> Accessed 1st February 2023, Section 65; HM Treasury (n 775), Pages 7-12.
[784] Chiu (n 100), Page 271.
[785] Johnstone (n 101), Page 261.

unpermissioned blockchain technology must be sought after to provide any practical form of protection. The next section will explore the possibility of self-regulation within the peer-to-peer method as a potential solution for legal redress of losses arising from systematic errors.

5.5: Self-regulation and Ostrom

As noted, the lack of redress for faults in unpermissioned blockchains is unlikely in itself to provide a sufficient risk to justify regulation. It is likely to be a matter left to self-regulation and this section will consider one possible model.

Systematic errors exist within unpermissioned blockchain technology which can create risk for users engaging with the technology. There is a lack of traditional legal protection for such end users in the current FCA approach.[786] To determine whether users may have the potential to adequately protect themselves, self-regulation necessitates analysis. The approach of Elinor Ostrom[787] will be considered as one possible way in which unpermissioned blockchain technology could have measures in place to self-manage. This will provide further indication as to the appropriate approach for systematic errors within unpermissioned blockchain technology.

Ostrom builds upon the traditional theory of the tragedy of the commons, which must first be discussed. "Therein is the tragedy. Each man is locked into a system that compels him to increase his herd without limit – in a world that is limited. Ruin is the destination toward which all men rush, each pursuing his own best interest in a society that believes in the freedom of the commons."[788] Hardin proposes that individuals pursue their own interests without consideration for society, thus resulting in societal

[786] For understanding into the advertising controls of crypto see, Financial Conduct Authority (n 569). For understanding of the warnings the FCA makes about crypto see, Financial Conduct Authority (n 113), Page 12.
[787] Ostrom (n 618).
[788] Garrett Hardin, 'The Tragedy of the Commons' (1968) 162(3859) Science 1243, Page 1244.

ruin, unless prevented.[789] Regulation and punishment are often viewed as possible solutions to correct this social (market) failure.[790] Within unpermissioned blockchain technology, the freedom of choice may need to be restricted to protect peer-to-peer users from the risk of systematic errors.

Ostrom famously challenges this theory and highlights that one of Hardin's misunderstandings is that he views individuals "as being trapped in this situation – largely because he did not envision that users could self-organize and devise institutions to extract themselves from tragic overuse."[791] Presuming that one is trapped and that society is incapable of self-management creates a need for external management.[792] If we suppose that self-ruin is evident, it is logical to suggest that in a natural resource setting only two viable options remain, privatisation or regulation.[793] Ostrom indicates that these options are not explicitly affirmed by evidence, but are merely presumptions.[794] No solution is perfect, each solution may have its own problems.[795] The presumption of ruin from self-management may justify regulation in many settings. Within unpermissioned blockchain technology the ruin could be the presumptions of criminal use and volatility of markets. Ostrom suggests that rather than leading to ruin, society can survive and potentially thrive under this self-preservationist system.[796] Within the context of unpermissioned blockchain technology, the network of users may

[789] Daniel Rankin, Katja Bargum and Hanna Kokko, 'The tragedy of the commons in evolutionary biology' (2007) 22(12) Trends in Ecology and Evolution 643, Page 643.
[790] Ibid.
[791] Elinor Ostrom, 'Tragedy of the Commons', in Steven N Durlauf and Lawrence E Blume (ed) *The New Palgrave Dictionary of Economics* (2nd edn Palgrave Macmillan 2008).
[792] For an interesting discussing in how the commons governance system operated successfully and did not reach tragedy see, Susan Jane Buck Cox, 'No Tragedy of the Commons' (1985) 7(1) Environmental Ethics 49.
[793] Ostrom (n 618), Page 9.
[794] This can also provide similarities to the 'nirvana fallacy' as referenced earlier. A presumption of a perfect solution is naïve and nothing more than a fallacy. See, Hantke-Dumas (n 687), Page 188.
[795] For a debate surrounding the idea of a single solution see, Ostrom (n 618), Pages 13-15.
[796] Ibid, Page 56.

be capable of self-management through code, including in relation to faults, and therefore it must be considered as an option.[797]

Ostrom signifies that the nature of natural resources and the management of them is complex and multi-faceted.[798] In circumstances where different parties are reliant or impacted by the natural resource, interdependency exists between all parties involved.[799] When applying this concept to regulation of unpermissioned blockchain, we can appreciate that there are numerous parties operating within the regulatory space[800] and they are interdependent but no one individual is essential or obliged to participate. Within unpermissioned blockchain technology, peer-to-peer users work interdependently to ensure maintenance of the network but are not obliged to.[801] Any proposed "regulatory approach" must consider the impact on the variety of stakeholders within unpermissioned blockchain technology.[802] This can be linked to the discussion throughout this chapter whereby a single uniform approach to regulation is regarded as impossible and unpredictable.[803]

[797] Ostrom highlights that one way for a common goal to be pursued without regulation is through contract. (See Ostrom (n 618), Page 15). It has already been recognised that within the exchange-based model the use of contract seems like an adequate solution. However, the same cannot be said for systematic errors within the peer-to-peer form of unpermissioned blockchain technology.
[798] Ostrom (n 618), Page 2.
[799] Ibid, Page 38; Geetika Jain and others, 'Blockchain for SME Clusters: An Ideation using the Framework of Ostrom Commons Governance' (2022) 24 Information Systems Frontiers 1125, Pages 1128-1129.
[800] For further discussion see, Terrence Daintith, 'A Regulatory Space Agency' (1989) 9(4) Oxford Journal of Legal Studies 534, Page 543; Morgan and Yeung (n 649), Page 59; Leigh Hancher and Michael Moran, *Organizing regulatory space* (1989) as found in Robert Baldwin, Colin Scott and Christopher Hood, *A reader on Regulation* (Oxford University Press 1998), Page 153.
[801] As discussed previously (see section 1.2.1), liability imposed on a specific role may cause an unfair outcome. For example, 'miners' should not be liable for coding errors.
[802] Hardin suggests this can only be achieved through external intervention. Whereas Ostrom postulates that there is potential for the stakeholders themselves to have social awareness.
[803] Due to the complexity of social, economic and legal elements. This touches on Morgan & Yeung's socio-legal view that society must be considered and the recognition of numerous forms of governance. See, Morgan and Yeung (n 649), Page 4.

Ostrom suggests that eight requirements may exist for self-preservation to be realised and here we can identify where this approach may not be suitable for self-regulation of unpermissioned blockchains.[804]

(1) Roles and boundaries must be clearly defined.[805] The rights parties have to withdraw from the common resource and the precise location of that resource must be explicitly clear. There is a critique of this point that by placing any restriction on a common pool of resources you effectively create private property which may contravene the idea of the commons.[806] However, this notion of boundaries refers to a common access whereby individuals may have different levels of removing from the resource. This is likely to be satisfied in the peer-to-peer model as users can withdraw at any time and roles of miners for examples are clearly defined through coding. Although, due to the lack of obligation to perform such a role, responsibilities may not be defined clearly. Shared responsibility has the possibility that no party will do what is necessary which could limit the ability to self-manage.[807] However, it is likely that incentivisation of roles can mitigate this issue to ensure that roles are somewhat defined and operational.[808]

(2) Rules cannot be generic and must be specific to the location.[809] Governance must be customised to ensure practicality and be influenced by cultural and societal aspects. This could be achieved for example through a formal contract between parties which is to be amended regularly.[810] Such a formalised rule setting system in the form

[804] Andrea Pia, 'Ghosts in the shell: The promises of water users' associations and the double life of Elinor Ostrom's design principles in rural China' (2023) 30(1) Journal of Political Ecology 62, Page 67. These eight requirements were evident in the successful examples of 'self-preservation' that Ostrom explored.
[805] Ostrom (n 618), Page 91.
[806] Walter Block and Ivan Jankovic, 'Tragedy of the Partnership: A Critique of Elinor Ostrom' (2016) 75(2) American Journal of Economics and Sociology 289, Page 294.
[807] For a discussion of the shared responsibility of maintenance and how this may impact liability see, Hong Kong Monetary Authority (n 66), Pages 103-104.
[808] For a discussion of the incentivisation present in unpermissioned blockchain technology see, Shrestha, Vassileva and Deters (n 441).
[809] Ostrom (n 618), Page 92.
[810] Block and Jankovic (n 806), Page 297.

of contract would be unlikely in the peer-to-peer method due to the likely lack of intention to be contractually bound,[811] the decentralised nature[812] and the presence of anonymity.[813] Determining any form of specific rules can be difficult to gauge as the internal rules appear to be more akin to conventions or expectations rather than strict rules.[814] However, the coding would surely be more precise.[815]

(3) Stakeholders must be able to have some aspect of participation in rule-setting/rule-changes.[816] This is a key principle for the perspective of compliance and future development of the resource.[817] Whether this is through consultation or more stringent processes, various stakeholders must feel that their opinion is valued. One could liken this to the concept of a partnership whereby decisions are made collectively.[818] This principle of rule-setting is also seemingly satisfied in the peer-to-peer model through voting and forking processes.

(4) Monitoring.[819] There must be some oversight to the way the rules are being applied. The resource itself must be monitored but also the behaviour of users as this can feed into the following principles by recognising when behaviour may need to be punished.[820] Punishment is a complex issue and will be discussed in the next principle of sanctioning, but the monitoring element may be possible. This requirement of monitoring could fall under the aspect of cryptography. Theoretically the mining process holistically could operate as the monitoring feature by limiting rule-breaks and so this principle can be said to be present in the peer-to-peer method.

---

[811] Ghosh (n 460), Chapter 34, Page 1.
[812] Financial Conduct Authority (n 113), Page 9.
[813] Houben (n 60), Page 263. See also the discussion in 2.2.
[814] Salmon and Myers (n 255), Page 4.
[815] For a discussion on whether the coding itself is an appropriate system of governance see, Yeung (n 254).
[816] Ostrom (n 618), Page 93.
[817] Sait Sarr, Bunny Hayes and Daniel DeCaro, 'Applying Ostrom's Institutional Analysis and Development framework, and design principles for co-production to pollution management in Louisville's Rebbertown, Kentucky' (2021) 104 Land Use Policy, Article 105383, Page 2.
[818] Block and Jankovic (n 806), Page 294.
[819] Ostrom (n 618), Page 94.
[820] Sarr, Hayes and DeCaro (n 817), Page 2.

(5) Sanctions.[821] In order for the monitoring to be successful, sanctions must be suitable for the seriousness of the rule breach.[822] Whether a sanction is perceived as fair or not can impact the adherence to the rules themselves. However, it is unlikely that any "sanctioning" system could be effectively implemented in the peer-to-peer method of unpermissioned blockchain technology. This is largely due to the permanence of the ledger and lack of centralised authority.[823] Thus, the system's ledger cannot be altered after any changes. Additionally, issues of anonymity can be relevant when seeking to determine who has breached a rule and what punishment is necessary. It is well-recognised how anonymity can provide a barrier to enforcement of traditional law,[824] however, the same is likely to be true for any internal self-management system of governance.

(6) There must be an internal redress system.[825] In order to resolve conflicts, there needs to be an appropriate and fair system which is quick and efficient.[826] Similar to requirement (5), (6) seems to not be present in the peer-to-peer method. Due to the trust in the code and the expectation of immutability, there is no expectation for error.[827] Therefore, there appears to be a lack of an internal conflict resolution system.

(7) "Minimal recognition of rights to organise".[828] This means that whilst there needs to be freedom from external intervention, the state must grant sufficient power (recognition) to those who seek to self-manage. Without state support it is difficult for the individuals to effectively govern. This could be suggested to exist within

[821] Ostrom (n 618), Page 94.
[822] Rankin, Bargum and Kokko (n 789), Page 643.
[823] Roberto Domingos Taufik, 'Block Change: The Fallacy of Blockchain Immutability and Cartel Governance' (2020) 1 Notre Dame Journal on Emerging technologies 307, Page 311; Hong Kong Monetary Authority (n 12), Page 16.
[824] Zetzsche, Buckley and Arner (n 141), Page 1392; Houben (n 60), Pages 263-264
[825] Ostrom (n 618), Page 100.
[826] Failure to do so would be detrimental within natural resources.
[827] Roberto Domingos Taufik, 'Block Change: The Fallacy of Blockchain Immutability and Cartel Governance' (2020) 1 Notre Dame Journal on Emerging technologies 307, Page 311; Hong Kong Monetary Authority (n 12), Page 16.
[828] Ostrom (n 618), Page 101.

unpermissioned blockchain technology as there is limited legal intervention currently. Whilst the intervention is restricted, the recognition is not evident. The level of recognition can vary but some acknowledgement of the right to self-govern can be important.[829] Without this legitimate legal foundation it will be difficult for the group to ensure compliance. In the English legal system, the approach has been cautionary. As a result, no "recognition" has been made to the validity of self-management of unpermissioned blockchain technology. In accordance with Ostrom, this may provide a stumbling block for potential self-regulation. If regulators were to provide such recognition and seemingly accept self-governance of the blockchain this does not negate the potential for more traditional regulation in the future. In accordance with Ayers and Braithwaite's responsive regulation concept,[830] regulators can retain oversight over the industry and as the technology develops and further understanding is gained, could transition from self-regulation to "more formal legal regulation"[831] over the coming years only if it is deemed necessary.

(8) "Nested enterprises".[832] This means that there must be multiple layers to the organisation.[833] Aspects of monitoring and conflict resolution for example must be defined within their own department within the organisation. There must be a degree of separation and a degree of overlap to achieve fairness and efficiency. Gazi and others regard Ostrom's eight requirement as the core aspect of a self-management system, stating that responsibilities must be structured in a tiered governance structure.[834] They argue that this requirement could be achieved in an unpermissioned blockchain system

[829] Yahua Wang, Minghui Zhang and Jingning Kang, 'How does context affect self-governance? Examining Ostrom's design principles in China' (2019) 13(1) International Journal of the Commons 660, Page 682.
[830] Ayers and Braithwaite (n 656).
[831] Howell and Potgieter (n 131), Page 1.
[832] Ostrom (n 618), Page 101.
[833] Eduardo Araral, 'Ostrom, Hardin and the commons: A critical appreciation and a revisionist view' (2014) 36 Environmental Science & Policy 11, Page 15.
[834] Gazi and others (n 128), Pages 1 and 3.

if there are tiers of commitment rules and tiers of incentivisation to match those requirements from the outset of the platform's development.[835] However, some of the suggestions they make such as registration of users, agreeing to governance duties and differing rights of users could be perceived as adding centralised elements into a decentralised governance system. Gazi and others recognise this but merely state that such principals "should be curated carefully to avoid to problem of unintended centralization",[836] but do not explain how this may be achieved. In the proof-of-stake validation method proposed by Gazi and others,[837] one issue with this tiered structure of responsibilities and incentives is that a decentralised community will only focus on some of these tiers due to greater incentive potential which may impact the performance of the platform. Although, as argued by Gazi and others, issues of incentivisation are present in any unpermissioned blockchain technology system,[838] such a tiered system may further these issues by creating them on each tier of responsibilities.

Whilst it may be possible for a platform to develop in the manner raised above, it is difficult to argue that a platform using unpermissioned blockchain technology presently can be described accurately as having multiple layers to its organisational structure.[839] The key issue here is the difficulty of establishing a hierarchy of users.[840] The lack of centralisation creates a reliance on incentivisation to ensure the operation of the platform.[841] The organisational structure of unpermissioned blockchain technology

[835] Ibid. For further discussion of this proposed tiered governance structure within unpermissioned blockchain technology see, Gazi and others (n 128), Pages 15-20.
[836] Ibid, Page 20
[837] Ibid Pages 1 and 3.
[838] Ibid, Pages 12-13. For a discussion of the incentivisation present in unpermissioned blockchain technology see, Shrestha, Vassileva and Deters (n 441).
[839] For a discussion of the benefits of this proposed tiered governance structure within unpermissioned blockchain technology see, Gazi and others (n 128), Pages 21-22.
[840] See the discussion of the difficulty of determining a hierarchy of users in section 1.3.1; Hong Kong Monetary Authority (n 66), Page 104.
[841] For a discussion of the incentivisation present in unpermissioned blockchain technology see, Shrestha, Vassileva and Deters (n 441).

is highly unconventional and so does not currently appear to conform to the concept of multi-layered organisation.[842]

As a result, all 8 requirements are not evident within the peer-to-peer model of unpermissioned blockchain technology. By using Ostrom's principles to inform regulation, it could be suggested that self-management in the form of self-regulation is not ideal within unpermissioned blockchain technology and a different approach may be needed. Other approaches may also face difficulties, as the failed experiment of the DAO illustrates.[843] Originally created in 2016 as a decentralised crypto-focused venture capital fund, it saw prominent success initially.[844] However, coding errors resulted in cryptocurrency being stolen and consequent protection measures that were sought within the system resulted in breaches of American Federal law.[845] Seven years on and the DAO experiment is the example of all that can go wrong in this sphere if self-regulated.[846] Decentralised platforms and technologies may consequently struggle to self-manage as alluded to in the discussion of Ostrom above.

There has been the suggestion that Ostrom's self-management theory will only be successful for smaller pools of resources that are to be managed locally, whereas Hardin's view of the commons is more applicable to large scale resources.[847] Currently, the limited scale of usage of cryptocurrencies in the UK[848] may have suggested a potential for application of Ostrom's theory. However, it is clear than not all the

[842] See the discussion of the difficulty of determining a hierarchy of users in section 1.3.1; Hong Kong Monetary Authority (n 66), Page 104.
[843] Samuel Falkon, 'The Story of the DAO – Its History and Consequences' (December 2017) <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee> Accessed 1st February 2023.
[844] Ibid.
[845] Ibid.
[846] Brian Sanya Mondoh and others, 'Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion?' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144753> Accessed 1st February 2023; Peder Ostbye, 'Exploring The Role of Law in The Governance of Cryptocurrency Systems and Why Limited Liability DAOs might be a Bad Idea' (January 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007547> Accessed 1st February 2023.
[847] Araral (n 833), Pages 11-12.
[848] HM Treasury (n 120), Pages 8-9.

elements would be evident in the peer-to-peer method. Therefore, it could suggest that due to the supranational nature of unpermissioned blockchain technology[849] and the increasing usage,[850] that self-management may be impractical.

A key distinction to reiterate however, is that Ostrom is not debating self-regulation or self-preservation more broadly. Ostrom focuses primarily on the governance of a natural resource. Even within the context of natural resources, many factors can impact the applicability of these principles such as the size of the community and the dependency of that group on the resource.[851] Unpermissioned blockchain technology is not a natural resource and so there may be more flexibility in what is required to self-manage. Nevertheless, Ostrom's theory suggests very important social aspects for the acceptance of self-management. Failure to adhere to these can leave unpermissioned blockchain technology with a degree of vulnerability from a self-regulation perspective. However, under Ostrom's principles it is unclear whether all eight requirements are necessary.[852] Consequently, it may be sufficient that unpermissioned blockchain technology possesses the potential to display some of these requirements of self-management from Ostrom. As mentioned throughout this chapter, there seems to be no perfect solution to self-regulation of unpermissioned blockchains, yet the level of public risk presented is as yet too low to merit more interventionist forms of regulation.

5.6: Conclusion

This chapter recognises that the meaning of regulation impacts the determination of its justification.[853] The traditional "command and control" approach views regulation

[849] Bjelajac and Bajac (n 54), Page 22.
[850] HM Treasury (n 120), Pages 8-9.
[851] Wang, Zhang and Kang (n 829), Page 674.
[852] This is important to note especially as we have applied the theory to unpermissioned blockchain technology and not a natural resource. This broader application would suggest a greater degree of flexibility.
[853] Baldwin, Cave and Lodge (n 62), Page 3.

in a manner which is warranted by a strong public need.[854] The present level of usage of cryptocurrencies in England and the interaction with unpermissioned blockchain technology is minimal,[855] which may suggest a lack of such public need. If the public need eventually requires further protection than is offered in the current approach, then a range of policy choices exist.[856] The UK government acknowledges the necessity of a flexible and adaptive approach to regulation and so the potential to change the current approach remains.[857]

If regulation is viewed in a broader manner through decentred regulation, the range of regulatory options and the possibility for justification is increased.[858] The most applicable justification is risk itself.[859] However, the limited use of unpermissioned blockchain technology and cryptocurrency mean that the less traditional forms of decentred regulation may be the only approaches that could be presently justified.

One less traditional decentred regulatory technique that was applied involved the use of Ostrom's governing the commons[860] as an analogy of the potential for self-regulation within the peer-to-peer method of transaction. The eight requirements that Ostrom views as a necessity for self-management of a natural resource were found to not currently be present within the structure of unpermissioned blockchain technology.[861] However, the nature of a natural resource and that of unpermissioned

[854] Black (n 622), Page 2. Selznick's definition would be another example of a definition within the 'central meaning'. See Baldwin, Cave and Lodge (n 62), Pages 2-3. For a discussion on the potential efficiency of the command-and-control approach see, Daniel Cole, 'When is Command-and-Control Efficient? Institutions, Technology, and the Comparative Efficiency of Alternative Regulatory Regimes For Environmental Protection' (1999) Wisconsin Law Review 887.
[855] HM Treasury (n 120), Pages 8-9.
[856] Chiu (n 100), Page 263.
[857] HM Treasury (n 120), Pages 10-11.
[858] Dimity Kingsford Smith, 'What is Regulation – A Reply to Julia Black' (2002) 27 Australian Journal of Legal Philosophy 37, Pages 39, 41 and 43; Black (n 622), Pages 3 and 4.
[859] Black (n 151), Page 304. Although the proof-of-work validation method does create wastage which may also justify regulation. See Baraniuk (n 315); Liana Badea and Mariana Claudia Mungiu-Pupazan, 'The Economic and Environmental Impact of Bitcoin' (2021) 9 IEEE 48091; Alex de Vries, 'Bitcoin boom: What rising prices mean for the network's energy consumption' (2021) 5(3) Joule 509; Anh Ngoc Quang Huynh and others, 'Energy Consumption and Bitcoin Market' (2022) 29 Asia Pacific Financial Markets 79.
[860] Ostrom (n 618).
[861] Ibid, Pages 91-101.

blockchain technology are not identical. Consequently, the presence of risk within unpermissioned blockchain technology creates the possible justification for a decentred form of regulation which may include self-regulation of the peer-to-peer method to provide the solution for the lack of legal redress for systematic errors within unpermissioned blockchain technology.

Chapter 6: Recommendations

This thesis focuses on the possibility of legal redress for systematic errors within unpermissioned blockchain technology, examining both whether it is practicable and whether further steps are needed to protect those who suffer loss because of such errors. Throughout the discussion in this thesis, it has been identified that the current contract and tort laws in England are unlikely to provide sufficient legal redress for systematic errors arising from unpermissioned blockchain technology. The main significance of this point is that it could undermine cryptocurrency investments, and this could cause unwitting consumers to suffer losses. The FCA have acknowledged that not only is there limited legal protection for errors within cryptocurrencies, but many users may not be aware of this.[862] This risk is one that regulation might address and at the time when this thesis was submitted a consultation exercise regarding future cryptocurrency regulation was announced, although it has not been possible to consider this consultation in detail. Hitherto, there has been the notion that unpermissioned blockchain and platforms such as Bitcoin are impossible to regulate.[863] There are unique legal problems that can arise from the use of such a novel technology that arguably make it "inherently almost impossible to regulate in the same way as other instruments."[864] However, there are also some potential unique solutions that can bring greater prospects of legal redress and legal clarity within this field.

Blockchain technology is certainly a key technological advancement and has significant potential to impact many industries and societal norms.[865] It could be stated that the question is not whether society will embrace the technology, but how this will

[862] Financial Conduct Authority (n 113), Page 12.
[863] Howell and Potgieter (n 131), Page 1.
[864] Ibid.
[865] Bodo, Gervais and Quintais (n 328), Page 312.

be manifested.[866] Partly this will require adaptation in the law and this chapter will contribute to discussion of how this can be achieved. Accordingly, as the technology continues to infiltrate into society, these recommendations can provide key guidance for how the regulatory landscape should develop.

This chapter will focus on the key recommendations that could increase the potential for legal redress for systematic errors, within a broader framing of cryptocurrency and crypto exchange regulation and will be directed at regulators as a general guide which can be used to develop the regulatory landscape moving forward. The recommendations provided are not discussed in order of importance. Although some recommendations may hold more weight than others, much of this significance will depend on the manner of future adoption of the technology. From the perspective of legal redress for systematic errors in unpermissioned blockchain technology, these are the key recommendations that would need to be implemented for further clarity and legal redress to be present.

6.1: Clarity of legal approach to unpermissioned blockchain technology

As discussed in Chapter 4, contract and tort law in England is unlikely to offer protection to users for errors that can occur within unpermissioned blockchain technology[867] and this public risk has not yet caught the attention of regulators. Instead, much of the current regulatory approach has relied on restrictions on advertising[868] as well as warning users that risks are present in cryptocurrency investments[869] and that

[866] Hughes and others (n 171), Page 2; For a useful example of how blockchain has wider capabilities than just cryptocurrency, see Chris Baraniuk (BBC), 'Blockchain: The revolution that hasn't quite happened' (2020) <https://www.bbc.co.uk/news/business-51281233> Accessed 1st February 2023
[867] Yeoh (n 617), Page 202
[868] Financial Conduct Authority, 'Strengthening our financial promotion rules for high risk investments, including cryptoasset: Consultation Paper CP22/2' (FCA CP22/2 2022) <https://www.fca.org.uk/publication/consultation/cp22-2.pdf> Accessed 1st February 2023, Pages 46-51; Financial Conduct Authority, 'Strengthening our financial promotion rules for high-risk investments and firms approving financial promotions: Policy Statement PS22/10' (FCA PS22/10 2022) <https://www.fca.org.uk/publication/policy/ps22-10.pdf> Accessed 1st February 2023, Page 3
[869] Financial Conduct Authority (n 569)

there is minimal protection available.[870] This approach essentially results in users having to be willing to accept the risk if they want to interact with the platforms that use the technology.[871] One of the impacts of this is that with the limited legal protections available, it could be suggested that there is limited legal clarity, potentially impacting on consumer investors,[872] which could further some of the scepticism that surrounds the technology.

As mentioned in Chapter 5, among some theorists there is the view of markets being efficient and that any interference from states should be avoided.[873] However, there is also the idea that states can be considered a key stakeholder for any societal development in respect of their own willingness to adopt the change and the way they regulate the development.[874] Therefore, by not regulating unpermissioned blockchain, cryptocurrency, or the exchanges and DEX that enable transactions, nor implementing the use of blockchain technology at state level such as adopting the technology for the land registry,[875] it could exacerbate the uncertainty and volatility within the market.[876] Therefore, the key recommendation here is that further legal clarity is needed and the government consultation may be welcomed in this regard. Although informed investors may be able to adequately deal with the risk present in the cryptocurrency markets it is one of the many risks that consumer investors are unlikely to appreciate. As the technology continues to develop and the level of interaction by the public increases, and the ways in which they can transact alter, the risk increases. Without clear action from

[870] There are also plans to regulate stablecoins although this is beyond the scope of the liability discussed in this thesis. For more information on this see, HM Treasury, 'Government sets out plan to make UK a global cryptoasset technology hub' (April 2022) <https://www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub> Accessed 1st February 2023.
[871] Financial Conduct Authority (n 113), Pages 11-13.
[872] For a discussion of this in the context of smart contracts see, Nir Kshetri, 'Blockchain's roles in strengthening cybersecurity and protecting privacy' (2017) 41 Telecommunications Policy 1027, Page 1036.
[873] Baldwin, Cave and Lodge (n 62), Page 3.
[874] Sreejith Balasubramanian and others, 'A readiness assessment framework for Blockchain adoption: A healthcare case study' (2021) 165 Technological Forecasting and Social Change, Para 2.1.1.
[875] HM Land Registry (n 1).
[876] Financial Conduct Authority (n 113), Pages 11-13.

states moving forward, there is the problem that the level of harm suffered by users could increase significantly in the coming years without the legal protections to minimise the wider financial and societal impacts. Where states seek innovation and do not wish to ban developments such as unpermissioned blockchain technology or the platforms that utilise it, they must be prepared to drive and steer the policy and interaction in this field.

It was recognised in Chapter 4 that often with speculative financial activity there is an unwillingness by regulators to be active within the market and suggest what users should not do.[877] Often policies will be taken so that risk can be managed by the user themself rather than actively trying to protect against such risk.[878] It is recognised that this first recommendation would be a significant deviation from what would be considered as the norm within the financial market setting. However, it is a needed change as the risk has clearly not been managed effectively when considering: the volume of scams,[879] numerous hacks,[880] examples of poor governance,[881] possibilities of insider dealing and the problems of the DAO which sought to have decentralised governance through smart contracts.[882] Of course, regulation may not remove the possibility of harm in the market but may mitigate it.

[877] Chiu (n 100), Page 264.
[878] Financial Conduct Authority (n 569); Chiu (n 100), Page 264.
[879] For some examples see, Wilson (n 38); Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368. It is also relevant to note that further regulation and more developed approaches are being applied in this field more broadly but unpermissioned blockchain technology specifically has not been the focus of legal intervention.
[880] For useful summaries of some of the key hacks of exchanges, see Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368.
[881] Calhoun (n 548).
[882] Brian Sanya Mondoh and others, 'Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion?' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144753> Accessed 1st February 2023; Peder Ostbye, 'Exploring The Role of Law in The Governance of Cryptocurrency Systems and Why Limited Liability DAOs might be a Bad Idea' (January 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007547> Accessed 1st February 2023.

6.2: Divergence of legal approach and terminology

It is apparent from the discussion and analysis thus far that when considering the different methods of cryptocurrency transaction; the peer-to-peer method, the exchange-based method and the DEX method as examples, it is imperative that the law treats them as distinct methods but also that users are aware of this. This is crucial as the way the law can influence such methods is different thus impacting the potential level of protection.[883] Furthermore, users must be made aware that whether the platform they are using operates via permissioned or unpermissioned blockchain technology will significantly impact the applicability of a legal framework due to the presence (or lack) of a centralised party that liability can be attached to and also variations in the level of contractual underpinning for these blockchains.[884]

If this is not done, confusion is the likely result. There are two components to this. Firstly, an increase in education from state bodies could be needed. There has already been the acknowledgement from the FCA that users in this field may not be so aware of the technology and the risks concerned.[885] One potential solution to this is rather than just warning of the risks, to educate in the distinctions of the technology and how the methods of transaction differ from one another. This could be a necessary step in order "to ensure that those engaged in it are able to manage the risks of their activity".[886] The second component here is by treating them as separate avenues for legal regulation, further understanding could be derived from users that the varying methods of transaction must be viewed as distinct aspects and it is incorrect to speak of blockchain generally, as there are a number of elements that are highly dependent on the type of the technology and the method of transaction, including different types of cryptocurrency and different means of exchange.

[883] Ostbye (n 202), Page 17.
[884] Hong Kong Monetary Authority (n 12), Pages 20-21.
[885] Financial Conduct Authority (n 113), Page 12.
[886] Chiu (n 100), Page 263.

6.2.1: The peer-to-peer method

The recommendations in this chapter are based on the analysis of English law and the FCA's approach as at the end of January 2023, prior to the consultation exercise being announced. Although the recommendations are capable of wider applicability than solely the English legal system, political difference may inhibit truly global recommendations. For example, in states where Bitcoin and cryptocurrencies are banned,[887] there will be no need to increase the protection for users and there will be no desire to do so in countries where Bitcoin has been adopted as legal tender.[888]

It has already been highlighted throughout this thesis that unpermissioned blockchain technology and particularly the traditional method of transaction, the peer-to-peer method, poses unique problems for traditional legal systems.[889] Firstly, the technical make-up of the technology is unique and relies on the underlying coding and the hash code for example rather than a centralised party.[890] The trust is placed in the technology rather than a traditional intermediary and this is referenced in the whitepaper of Bitcoin for example.[891] This is one of the aspects that makes such a technology so revolutionary but also could render it incompatible with traditional legal systems.

The lack of a centralised party and the, theoretically, shared responsibility of maintenance of the network effectively removes a traditional hierarchical organisational

[887] For example, countries such as China, Bangladesh, Bolivia, Ghana and Mexico have effectively banned cryptocurrencies. 'Ban' is used in quite liberally, as some countries have an 'indirect ban' where trading Bitcoin is extremely difficult and inaccessible, but there is no explicit or direct ban. For an interesting discussion on the impact that such bans can have on trading values of cryptocurrency see Alexander Copestake, Davide Furceri and Pablo Gonzalez-Dominguez, 'Crypto market responses to digital asset policies' (2023) Economic Letters 222, Article 110949.
[888] For a discussion on El Salvador adopting Bitcoin as legal tender see, Fernando Alvarez, David Argente and Diana Van Patten, 'Are Cryptocurrencies Currencies? Bitcoin as a Legal Tender in El Salvador' (April 2022 – Revised February 2023) working paper 29968 <https://www.nber.org/system/files/working_papers/w29968/w29968.pdf> Accessed 1st February 2023. For a brief discussion of the Central African Republic also adopting Bitcoin see, (bbc.co.uk), 'Why the Central African Republic adopted Bitcoin' (June 2022) <https://www.bbc.co.uk/news/world-africa-61565485> Accessed 1st February 2023.
[889] Hughes and others (n 171), Page 7; Hari and Pasquier (n 184), Page 423.
[890] Hong Kong Monetary Authority (n 12), Page 20.
[891] Nakamoto (n 51).

structure.[892] In turn, this means it is practically impossible to attach blame or fault to specific users or types of users should an error occur. Therefore, systems which traditionally rely on the possibility of pinpointing fault, such as contract and tort, have limited applicability within unpermissioned blockchain.[893] Consequently, contract and tort may provide no practical form of legal redress for peer-to-peer users within the peer-to-peer model that suffer loss because of a systematic error, largely due to the presence of anonymity and the lack of intention to be legally bound.[894] Although the underlying technology is immutable, potential risks are still present within the peer-to-peer method which include scams,[895] hacking,[896] governance issues,[897] and possibilities of insider dealing as examples.

The blockchain system is heavily reliant on the underlying coding, and it can impact the future developments of the network itself.[898] This has led to Lessig's theory of "code as law" within unpermissioned blockchain technology.[899] This thesis agrees with this concept, as the technical nature of the system is not so easily compatible with legal frameworks. The coding is the most effective and essential component for unpermissioned blockchain technology in respect of its governance. It is the only

[892] For a brief discussion of how unpermissioned blockchain technology makes no reference to any hierarchy see, Hong Kong Monetary Authority (n 66), Page 104.
[893] Zetzsche, Buckley and Arner (n 105), Page 1405; Financial Conduct Authority (n 113), Pages 13-14.
[894] *Tulip Trading Ltd* v *Bitcoin Association for BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624, Paras [67], [75], [83], [93], [103] and [105]; Houben (n 60), Page 263; Sage (n 451), Page 473; Ghosh (n 460), Chapter 34, Page 1; Gregory Klass, 'Intent to Contract' (2009) 95 Va L Rev 1437, Page 1439; Dori Kimel, *From Promise to Contract: Towards a Liberal Theory of Contract* (Bloomsbury 2003), Pages 136-139.
[895] For some examples see, Wilson (n 38); Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368. It is also relevant to note that further regulation and more developed approaches are being applied in this field more broadly but unpermissioned blockchain technology specifically has not been the focus of legal intervention.
[896] For useful summaries of some of the key hacks of exchanges, see Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368.
[897] Calhoun (n 548).
[898] Yeung (n 254), Page 209.
[899] Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books 2006); Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999).

method of control within such a system. As a result, it appears to be the only effective way to govern the peer-to-peer method of transaction. Therefore, the recommended legal approach for the peer-to-peer method of transaction is recognising the self-regulation of the technology through its coding. Encouraging and recognising self-regulation especially as a market is still developing can be practical.[900] Encouragement could be provided through states adopting the technology themselves and acknowledging clearly that the peer-to-peer transactions will be left to self-regulate without any private law interference. This is logical as ultimately the success of the system and its continued development and maintenance is reliant on its appeal and successful operation.[901] As noted, the most compelling incentive for exchanges to ensure security is the threat to reputation; within unpermissioned blockchains, the incentive is the continued operation of the platforms and the cryptocurrencies that are based on them.[902] These incentives may lead validators and coders within such systems to develop and navigate the platforms accordingly and within the best interests of the masses otherwise the platform will either not be used anymore, or forks within the platform will occur and the number of peer-to-peer users will be split across the forked system.[903] It is potentially therefore an internal incentive to govern the platform appropriately and in a manner that is fair whilst maintaining the core values of the system and providing a true and informed understanding of the issues and solutions within such a platform. This understanding of the industry and practices is something that Howell and Potgieter suggest that "traditional regulatory agencies are ill-equipped to govern" as they lack such informed knowledge.[904]

[900] Howell and Potgieter (n 131), Page 5.
[901] Ibid.
[902] Ostbye (n 202), Page 18.
[903] Howell and Potgieter (n 131), Page 5.
[904] Ibid, Page 1.

Assuming there is an internal incentive to govern the platform fairly, this can also indicate why the traditional command-and-control approach to regulation[905] would not be a practical legal approach.[906] Command-and-control regulation is a governmental activity that involves the use of strict rules which have punishments attached.[907] A command-and-control form of regulation could have minimal impact as it would be likely to result in regulatory arbitrage as with the potential of anonymity and the ability to operate globally, any form of regulation could be evaded and so may have little to no impact.[908] It would not necessarily result in coding changes or changes in practice to how peer-to-peer users interact with the system, other than the potential legal ramifications if their identity became known.[909] This key power of the code cannot be overcome by law and so whilst there will remain regulatory oversight, self-regulation is arguably the most appropriate form of governance for peer-to-peer transactions.

It is also worth noting that self-regulation of a cryptocurrency such as Bitcoin which operates as a supranational platform is more likely to achieve a degree of global uniformity than regulators attempting to govern their own jurisdiction in differing manners.[910] Due to the cross-jurisdictional nature and capabilities of the technology, coders and other key groups within the peer-to-peer method may develop industry practices that result in a degree of commonality and uniformity across unpermissioned blockchain technology and the internal governance systems of different platforms.[911]

---

[905] Black (n 622), Page 2.
[906] Examples of the command-and-control approach in the context of unpermissioned blockchain technology would be in the form of outright bans or regulating the methods of transaction such as registration and disclosure for money laundering or taxation purposes. For a discussion on the potential efficiency of the command-and-control approach see, Daniel Cole, 'When is Command-and-Control Efficient? Institutions, Technology, and the Comparative Efficiency of Alternative Regulatory Regimes For Environmental Protection' (1999) Wisconsin Law Review 887.
[907] Jingxiao Zhang and others, 'The impact of environmental regulations on urban Green innovation efficiency: The case of Xi'an' (2020) 57 Sustainable Cities and Society, Article 102123, Page 2; Black (n 622), Pages 2-3.
[908] Chiu (n 100), Page 265.
[909] Fleischer (n 736), Page 229.
[910] Howell and Potgieter (n 131), Pages 5-6.
[911] For a discussion of how this may be present in the exchange-based method globally with respect to industry practices and terms and conditions see, Howell and Potgieter (n 131), Pages 5-6.

Additionally, we must understand how this can be achieved. Self-regulation inherently does not necessarily require state action or choice. However, Ostrom suggests that for self-management to be successful, states must provide power to such groups seeking to self-manage or recognise that such management is valid by not interfering. This is referred to as the minimal recognition of rights.[912] If such validity is not granted to a community seeking to self-manage, then their rights to self-regulate can be questioned and it can minimise the acceptance of any internal rules or internal redress systems. Criminal activity will continue to be monitored and regulatory oversight in respect of money laundering and terrorism funding for example will continue to be operational and develop in the coming years primarily in a more command-and-control manner. However, in respect of liability for systematic errors, a clear statement that the internal system of code as law will be accepted and not overruled would provide sufficient legal clarity and the minimal recognition of rights that could be needed to further develop the self-governance system through coding. As noted previously, this would be an example of Ayers and Braithwaite's responsive regulation model and would provide regulators with oversight of the industry which may allow a more seamless transition to more traditional regulation if and when it is deemed necessary.

Currently, the FCA have largely just warned of the risks and stated that cryptoassets are largely unregulated.[913] However, by recognising the self-regulation of platforms within unpermissioned blockchain technology, peer-to-peer users will be more cognisant that the only avenue for redress is internally within the system itself and through coding and there may not indeed be any form of internal redress present where faults occur. It would therefore be up to individual platforms as to whether they wish to

[912] Ostrom (n 618), Page 101.
[913] Financial Conduct Authority (n 113), Pages 11-13.

utilise alternative dispute resolution methods to address any potential faults or forks or resolve any disputes. In summary, the recommendation from this thesis with respect to the appropriate legal approach for liability for systematic errors within unpermissioned blockchains is self-regulation through coding. Whilst there are risks from a legal perspective, the FCA have shown that they can maintain regulatory oversight and intervene, when necessary, with respect to criminal activity within the field.[914]

6.2.2: Transactions through exchanges

For exchange-based transactions, it is recognised that contract law is likely to be sufficient for governing redress for systematic errors within exchange-based transactions. The presence of terms and conditions create the basis for a contractual agreement to govern disputes arising between the exchange customer and the exchange.[915] For example, reference can be made to governing law and the legal jurisdiction to govern disputes.[916] The problem for investors who suffer loss as a result of a fault in an unpermissioned blockchain on which the cryptocurrency is based is that often liability is limited significantly within the terms and conditions of exchanges, normally to the point that exchanges would need to act negligently for liability to befall them. Since faults in a blockchain or cryptocurrency which is based on it are not attributable to the exchange, the result is that there is very little legal protection for exchange-customers when systematic errors occur.[917]

If regulators wish to protect investors further, and this should be a desire of theirs when considering the limited legal protection and the degree of risk,[918] my recommendation is for the implementation or adoption of a licensing system for

[914] Financial Conduct Authority (n 511).
[915] For an example, Binance state that to the maximum extent of the law they remove liabilities whether express or implied, so far as the law provides binance.com (n 203), Part IV Section 1.
[916] Coinfalcon.com (n 271), (Jurisdiction and Applicable Law); okex.com (n 522), S13.19.
[917] Financial Conduct Authority (n 113), Page 16.
[918] Howell and Potgieter (n 131), Page 4.

exchanges. The primary focus of such a licensing system could be: to impose requirements for coins listed on the exchange, like Listing Rules for shares which protect investors;[919] to ensure enhanced coding and security standards for the exchanges; as well as to require the segregation of client assets.[920] However, it has been acknowledged that a licensing system is not without its flaws. Learning from the issues of the New York licensing system[921] and licensing system in Japan,[922] as discussed in section 5.4, there would need to be a streamlined application process and sufficient enforcement powers granted to the FCA should any issues arise.

In respect of the desire to increase the security protection within the industry, as mentioned previously, there is the concern that this will become nothing more than a tick-box exercise as it may be difficult to actually solve the issues in a nascent, novel and developing industry.[923] However, even if the only result is further scrutiny or discussions regarding industry practices and security processes, then this in theory could increase the level of protection overall. Regarding the segregation of client money/assets, this is a vital step that the UK government in their latest consultation on cryptoasset regulation acknowledge would be important for consumer protection[924] and would enhance accountability, protection, and clarity within the industry.[925]

[919] Section 73A Financial Services and Markets Act 2000 grants the FCA right to alter and update such listing rules which can be found here, Financial Conduct Authority, 'The Listing Rules' (January 2023) <https://www.handbook.fca.org.uk/handbook/LR.pdf> Accessed 1st February 2023.
[920] The SEC have stated they believe this may be a necessary step in this industry. See, Gensler (n 762).
[921] For some discussion of this, see Roberts (n 765).
[922] Howell and Potgieter (n 131), Page 5.
[923] Ibid.
[924] HM Treasury (n 120), Page 52.
[925] If The Financial Services and Markets Bill is passed, the broad definition of cryptoasset could further the regulatory remit of the FCA which may also increase accountability and protection within the industry. See, Financial Services and Markets Bill, (HL Bill 80) <https://bills.parliament.uk/publications/49063/documents/2625> Accessed 1st February 2023, Section 65; Elderfield (n 769).

Additionally the SEC in America has stated that segregation is a key regulatory step that must be considered moving forward.[926]

6.2.3: The DeFi or DEX exchanges

The DeFi or DEX method of exchange provides a further unique approach due to the hybrid nature of its operation.[927] Whilst in theory it is decentralised, practically there is sufficient control retained by the exchange company through voting rights, which effectively mean there is some degree of centralisation.[928] This then means it must be governed in a different manner to the peer-to-peer method or the exchange-based method. As this is a hybrid system it may be necessary that a hybrid approach is taken. This will be a difficult balance for regulators and will need to be developed accordingly over the coming years as further understanding of this method increases.[929] The recent consultation paper confirms this as there is an acknowledgment that DeFi platforms such as DEXs operate internationally with several entities involved in the operation of the platform and that the level of risk may be especially high considering the rapid growth.[930]

Such a hybrid approach could result in the technology being self-regulated akin to the peer-to-peer method, however, the companies that create the DEX may be required to gain a license to do such activity in the manner discussed above for the non-DEX exchanges. The intricacies of such a governing framework would certainly require adaptation over the coming years but would at least provide a starting point for the governance of this hybrid and unique method of transaction within unpermissioned

---

[926] Gary Silverman (ft.com), 'SEC explores segregating businesses at crypto exchanges' (April 2022) <https://www.ft.com/content/efb9e8d5-02c1-4727-a46d-5ad5d34fdf28?accessToken=zwAAAX_5QvO9kdPvuejVAsFHJ9OkbVrV00_fKA.MEYCIQDiRlUDzo2mVDseOKit0_QBjSUVvhmsjg78wP87y-YPqQIhAOJZTbUoZizbYBtQOGPTRKmNaAcnu54RpyVPDoLNhQcC&sharetype=gift?token=33cb1b11-1cd3-4ad9-8bcf-6b1aa24e9bad#comments-anchor> Accessed 1st February 2023.
[927] Johnstone (n 101), Page 169; Wilson and Westbrook (n 200), Page 1.
[928] Kruppa (n 93).
[929] Howell and Potgieter (n 131), Page 1.
[930] HM Treasury (n 120), Pages 66-67.

blockchain technology. This would be ideal as the International Organization of Securities Commissions (IOSCo) have suggested that the regulatory focus needs to be attached to these DeFi markets and the level of threat posed.[931] The UK government also seems open to a custom regulatory system for DeFi whereby specified activities require authorisation from the FCA.[932]

One issue with such a system and such a recommendation is it would be highly fact sensitive. Although there is the theory that due to voting rights, creators of the DEX may effectively control the development of the DEX, the level of control may differ from one DEX to another.[933] If in the future, voting rights were transferred to other parties, it may become less clear which party would be required to obtain the license. It would be difficult to indicate that above a threshold level a company would have control and influence over the development of the platform, but below such threshold they would not. This recommendation is a cautionary one as there is clear recognition that as this method of transaction develops, such a recommendation and regulatory approach would need to develop also.[934] Alternatively, there is the suggestion that regulation could focus on traditional exchanges or intermediaries that facilitate access to DeFi to mitigate risks present within the market such as the prevalence of security threats.[935] The best solution for regulating DeFi platforms such as DEXs remains unclear. However, it is imperative that such a regulatory framework is established as there is a clear amount of risk that is present within the DEX method of transaction; one which if left un-monitored could have serious repercussions for DEX customers and the decentralised-finance markets moving forward.[936]

[931] Kruppa (n 93).
[932] HM Treasury (n 120), Page 67.
[933] Ibid.
[934] Ibid, Pages 67-68.
[935] Ibid, Page 68.
[936] Kruppa (n 93).

6.3: Risk is sufficient to justify regulation

As discussed above, exchanges, whether of the traditional type or DeFi, appear to be on a state regulatory trajectory whereas unpermissioned blockchain more generally, and the applications on it, are subject to self-regulation.[937] The latter position could change in the event that the level of risk within unpermissioned blockchain technology was considered sufficient to warrant regulation being justified, as discussed previously.[938] It must be noted here that "regulation" is viewed in the decentred perspective whereby the range of regulatory options are broader and as such the range of justifications to "regulate" can be wider than traditional command-and-control by the state.[939]

As previously mentioned, there have been several hacks of exchanges, scams within cryptocurrencies and threats in DEXs which may suggest that risk within the methods of transaction of unpermissioned blockchain technology is high.[940] The FCA have recognised that this cryptocurrency industry is one that generates notable risk of financial loss and this is indicated even in their current approach where there is a warning of the risks involved and an acknowledgement that it current markets remain largely unregulated.[941]

Traditional approaches to regulation and traditional justifications do not conform easily with unpermissioned blockchain technology. For example, the justification of market failure warranting regulation is a tricky concept to align with unpermissioned blockchain technology as it is difficult to determine the parameters of the market itself

[937] HM Treasury (n 120), Page 66.
[938] Black (n 151), Page 304.
[939] Walter Johnson, 'Flexible regulation for dynamic products? The case of applying principles-based regulation to medical products using artificial intelligence' (2022) 14(2) Law Innovation and Technology 205, Page 216; Black (n 622), Page 26.
[940] For some examples see, Wilson (n 38); Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; Yanaga Masao, 'Virtual currency-regulation and challenges in Japan' (2017) 32(7) Journal of International Banking Law and Regulation 283; Zetzsche, Buckley and Arner (n 141), Pages 1367-1368.
[941] Financial Conduct Authority (n 113), Pages 11-13.

and the key players and stakeholders within such a market to be regulated.[942] This is largely due to the decentralised nature of the technology whereby responsibility of maintenance and upkeep of the platform is theoretically shared equally amongst peer-to-peer users and further complicated due to the level of anonymity present. This is also partially due to the concept of "regulation" often being more constricted to the command-and control approach which involves strict rules being attached to specified parties by the state.[943] Additionally, any attempts to regulate through the command-and-control approach is going to be difficult especially in unpermissioned blockchain transactions as the anonymity and decentralised nature of the technology limits the effectiveness of rules that are designed to force a change in behaviour. As Morgan & Yeung suggest, this traditional approach may not always be an effective tool in behaviour modification especially when community interests may be more difficult to understand.[944] Unpermissioned blockchain technology could be considered an example of this type due to the decentralised nature and the numerous methods of transaction. Some even argue that the newer methods of transaction such as DEX create further risks for users.[945]

Therefore, this recommendation states that regulators need to approach "regulation" of unpermissioned blockchain technology in a wider manner. This is a unique technology and poses complex legal issues and so this will require a re-consideration of how regulators view regulation and the strict approach of justifications.[946] By viewing regulation in a decentred perspective, the range of regulatory approaches is broader and as such the threshold of justification can be

[942] Baldwin, Cave and Lodge (n 62), Page 16.
[943] Jingxiao Zhang and others, 'The impact of environmental regulations on urban Green innovation efficiency: The case of Xi'an' (2020) 57 Sustainable Cities and Society, Article 102123, Page 2; Black (n 622), Page 2.
[944] Morgan and Yeung (n 649), Page 4.
[945] Howell and Potgieter (n 131), Page 3.
[946] Ibid, Page 2.

lowered.[947] Further discussions surrounding DAOs,[948] the role of social media in encouraging speculative cryptocurrency investments[949] and education of users in this sector can all be important. This is a vital recommendation for the regulatory landscape moving forward. As identified in Chapter 5, the traditional approaches to regulation and traditional legal frameworks such as contract and tort are effectively incompatible within the peer-to-peer method of unpermissioned blockchain technology as much of these frameworks relies on the ability to pinpoint fault, which is a complicated and multi-layered issue within such a novel technology.[950]

By moving away from this traditional legal approach, and viewing regulation in a broader decentred manner, regulators will be able to approach the governance of unpermissioned blockchain technology with a set of fresh eyes and will be more capable to reach a governance strategy that is informed by the technology, industry and the future developments. The current level of risk with relatively minimal engagement suggests that a non-interventionist approach might presently suffice but there is the potential of enhanced risk should more individuals interact with the technology and its current platforms.[951] Failure to govern such technology and the liability implications could cause serious issues societally and economically if further adoption of such technology or cryptocurrencies occurs within the coming years.

[947] Black (n 622), Pages 2-4; Walter Johnson, 'Flexible regulation for dynamic products? The case of applying principles-based regulation to medical products using artificial intelligence' (2022) 14(2) Law Innovation and Technology 205, Page 216; Dimity Kingsford Smith, 'What is Regulation – A Reply to Julia Black' (2002) 27 Australian Journal of Legal Philosophy 37, Pages 39, 41 and 43.
[948] For further discussion of DAO governance see, Brian Sanya Mondoh and others, 'Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion?' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144753> Accessed 1st February 2023.
[949] For further discussion of the role of social media in cryptocurrency see, Feng Mai and others, 'How Does Social Media Impact Bitcoin Value? A Test of the Silent Majority Hypothesis' (2019) 35(1) Journal of Management Information Systems 19.
[950] Hong Kong Monetary Authority (n 66), Page 86.
[951] Hari and Pasquier (n 184), Pages 423 and 445.

6.4: A pro-active approach is needed

The previous recommendations have emphasised the need for a pro-active approach. The current regulatory approach in England has hitherto seemed rather reactive in respect to liability for systematic errors. Currently, peer to peer transactions on unpermissioned blockchains are not a big enough market to warrant a pro-active approach. However, as stated throughout this thesis, the potential of unpermissioned blockchain technology exists.[952] With the risks that are present, and the potential for usage, there is the possibility for the risk to increase and the impact to grow. The current reactive approach could leave a serious gap and potential issue for the individuals involved and the economy on a wider scale if usage can increase.

There is a theory that unpermissioned blockchain technology will not be adopted on a wider scale as the lack of centralisation is not appealing to organisations and bodies that currently have the control in society and will not want to relinquish it, for example any companies adopting blockchain technology, banking systems or state bodies within industries.[953] Although this is likely to be true, the potential for individuals to adopt platforms using unpermissioned blockchain technology exists, as illustrated by Bitcoin. There is also a growing social desire to challenge the infrastructure and the norms within the society. If this approach starts focusing in on the financial industry and more individuals start adopting these cryptocurrencies, companies will be forced somewhat to start accepting it more commonly as a means of payment and then the use of these cryptocurrencies and the risk will grow exponentially.[954]

This may be a hypothetical threat; however, the potential exists, and the concern is that if a reactive approach remains then the threat and potential for damage will be

[952] For more uses of blockchain see Xu, Weber and Staples (n 3); Sean Williams (Fool.com), '20 Real-World Uses for Blockchain Technology' (2018) <https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx> Accessed 1st February 2023. Although many of these examples relate to permissioned blockchain technology, the potential for use of unpermissioned blockchain technology remains a way to challenge current balances of power in many industries.
[953] Howell and Potgieter (n 131), Pages 6-7.
[954] Ibid.

significant. There is a theory that further legal clarity will stabilise the industry and provide a regulatory framework that can be adapted and altered accordingly depending on future developments in the industry. By trying to clarify the regulatory landscape now it will put regulators in a better position, one which will be more prepared and informed if the potential of the technology is realised, and further usage is adopted by individuals.

This would involve a policy choice shift from the current approach.[955] It could be argued that such a shift would be unlikely as the FCA seem satisfied with their reactive approach. This may be largely due to the level of investment in cryptocurrency being comparatively low and there being no present threat to the fiat currency.[956] However, the recommendation is that such a policy change would be a logical shift and would increase protection to users currently within the field but also provide an enhanced safety net should use increase significantly in the coming years. Although it is also recognised that this pro-active approach would not necessarily remove all risk or minimise the level of risk that is present but would provide further legal protections for such risk.[957]

6.5: Encouragement of permissioned blockchain technology

The fifth recommendation within this thesis is that there should be the encouragement of permissioned blockchain technology. As referenced at the beginning of this chapter, the distinction between permissioned and unpermissioned blockchain technology is important. Being apprehensive of blockchain technology overall is illogical if such apprehensions are derived from the perception of unpermissioned blockchain technology only. Permissioned blockchain technology provides a technologically advanced ledger system which can increase efficiency and be a useful

[955] Chiu (n 100), Page 271.
[956] Bank of England Financial Policy Committee (n 118), Page 2.
[957] Chiu (n 100), Page 265.

asset in many industries.[958] Due to the structure of permissioned blockchain technology, it allows a central party to retain control and oversight over the platform which increases its likelihood of adoption in many industries.[959]

There has already been reference to Maersk's successful use of blockchain technology and the recommendation here is that governments need to utilise the technology and encourage use within various markets.[960] In theory, governmental use of such technology will increase confidence and support of the technology. If more individuals use permissioned blockchain technology, this is better from a liability perspective in comparison to unpermissioned blockchain technology.[961] This is largely because the obstacles to legal redress that are present within unpermissioned blockchain technology and many of the risks that are also present, would not be present in permissioned blockchain technology.

Additionally, the centralised nature of permissioned blockchain technology increases the compatibility with fault-based liability systems, through a sounder footing in contract or tort, which would make legal enforceability easier in comparison with unpermissioned blockchain technology.[962] Some would state that blockchain technology is a revolutionary technology and one which will be used for years to come. If this is the case, it is important that permissioned blockchain platforms are well established and successful as this could mitigate the use and problems which would be created if further

[958] For insight into the number of industries that could be changed by blockchain see, cbinsights.com, 'Banking is only the beginning: 65 big industries blockchain could transform' (9th March 2022) <https://www.cbinsights.com/research/industries-disrupted-blockchain/> Accessed 1st February 2023.
[959] For a brief explanation of this see Blockchain Council, 'Permissioned and Permissionless Blockchains: A Comprehensive Guide' < https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/> Accessed 1st February 2023.
[960] Maersk is an international shipping logistics company. Together with IBM they launched a "digital shipping platform" (Toft Madsen (n 351)) in 2018 that was made possible with Permissioned blockchain technology.
[961] For a brief discussion on the comparison of accountability in unpermissioned vs permissioned blockchain platforms see, Howell and Potgieter (n 131), Pages 8-9.
[962] This is a similar point when comparing the exchange-based method of interaction with the peer-to-peer method of interaction; the presence of the central party/intermediary increases legal enforceability. For further discussion of this see, Ostbye (n 202), Page 17.

use of unpermissioned blockchain technology develops in the coming years. Further use of permissioned blockchain technology can help to develop the knowledge of the industry and the distinction between permissioned and unpermissioned blockchain technology. This could result in users being more informed and aware of the risks present.

6.6: A responsive approach

The final recommendation is that whilst a pro-active approach has been suggested, it is likely that any regulatory framework will need to adapt over the coming years. This is something that can be seen in global regulation with governance of the cryptocurrency industry becoming a focus within the EU, the US, the UK and South Korea as some examples; although the particular focus differs.[963] This developing regulatory landscape is not the only change that is likely in the coming years. The blockchain landscape is also likely to alter and evolve significantly and there remains a lot that is unknown but a lot of potential, nonetheless. Further adoption of smart contracts could be present in many industries which will require principles of contract law to be adapted and applied flexibly to the smart contracts.[964] New blockchains and different validation methods are likely to be implemented further.[965] The Ethereum blockchain was recognised as a significant advancement from the Bitcoin blockchain for example and it is possible that further developments will be made in the future,[966]

[963] For further discussion of some of these developing and changing approaches see, Howell and Potgieter (n 131), Pages 9-11.
[964] Law Commission, *Smart Legal Contracts Advice to Government* (Law Com No 401, 2021) Paras 4.91-4.92.
[965] For example, proof-of-stake can be regarded as a new alternative to proof-of-work as a validation practice. For further discussion on proof-of-stake see, Hari and Pasquier (n 184), Page 427.
[966] Andreas Bogner, Mathieu Chanson and Arne Meeuw, 'A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain' IoT'16: Proceedings of the 6th International Conference on the Internet of Things (November 2016) 177 <https://doi.org/10.1145/2991561.2998465> Accessed 1st February 2023. For further potential uses of the Ethereum blockchain see, Emre Yavuz and others, 'Towards secure e-voting using ethereum blockchain' (2018) 6th International Symposium on Digital Forensic and Security (ISDFS) <https://ieeexplore.ieee.org/abstract/document/8355340> Accessed 1st February 2023.

not least to address real concerns regarding the environmental cost of proof-of-work verification, as well as the concentration of mining around a decreasing pool of miners.

There has also been the increased use of cryptocurrency as a payment method and for blockchain based assets that five years ago were unknown, such as Non-Fungible Tokens (NFTs).[967] As this market develops and other creations are made, cryptocurrency could be an ever more necessary digital currency to own.

Additionally, there has been the suggestion that the world accounting system could be replaced by permissioned blockchain technology and centrally backed e-money moving forward. Dr Pippa Malmgren, a former US presidential advisor and economist stated whilst speaking at the World Government Summit 2022,[968] "we're about to abandon the traditional system of money and accounting and introduce a new one…The new accounting is what we call blockchain."[969] In doing so, she goes on to state that blockchain provides an almost perfect record of accounting and will enable further clarity to be determined on what is truly happening within an economy.[970] However, Malmgren also suggests that such a development is not without concern, and in the coming years there will be questions regarding the dangers of the balance of power between states and citizens.[971] The main point to raise here is that the potential of blockchain is far-reaching and the landscape of its use and societal impact is likely to alter significantly in the coming years.

---

[967] Foteni Valeonti and others, 'Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs)' (2021) 11 Applied Sciences 9931 <https://www.mdpi.com/2076-3417/11/21/9931#cite> Accessed 1st February 2023; Maria Demertzis, 'Non-fungible tokens (NFTs): The next chapter in crypto' (January 2022) Bruegel-Blogs <https://go.gale.com/ps/i.do?id=GALE%7CA690531927&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=&p=AONE&sw=w&userGroupName=anon%7Ed2a2fd82> Accessed 1st February 2023.
[968] For more information on this summit see, worldgovernmentsummit.org, 'home' <https://www.worldgovernmentsummit.org/events/annual-gathering-2022> Accessed 1st February 2023.
[969] TheTruthDrops, 'World Government Summit 2022: Dr Pippa Malmgren Talks About Blockchain & Digital Currencies' (2nd April 2022) <https://www.youtube.com/watch?v=cvXdSvja-aI> Accessed 1st February 2023.
[970] Ibid.
[971] Ibid.

With such developments, as alluded to by Malmgren, further risks and concerns will arise. If the landscape is likely to significantly alter in the coming years, there may be a temptation from regulators to wait and be reactive. However, as suggested in recommendation four, a pro-active approach is needed to provide legal clarity and a legal framework which can adapt in-line with future developments. Failure to do so, could lead to further risk and harm if use of blockchain technology (permissioned and unpermissioned) increases significantly, without clarity on how the law will govern and engage in such developments.

6.7: Summary

In summary, a pro-active approach which recognises the limitations of regulators is needed. It is vital that the regulatory approach does not attempt to significantly alter the nature of unpermissioned blockchain technology as this could minimise the industry's development and could result in further confusion for its users.[972] A clear legal approach which recognises the different methods of transaction as fundamentally distinct from one another and attempts to govern them accordingly is desired. It is imperative that it is not the technology itself that is regulated and governed but the activity that it produces in the varying methods of transaction.[973] In order to practically govern the novel legal issues posed by the uniqueness of unpermissioned blockchain technology there must be a reassessment of regulation itself. Regulators must move away from any pre-conceived notions of the technology or the meaning of regulation and must approach it in a new manner, one which views regulation as decentred and understands that the current methods of transaction produce risks, not the technology itself.[974]

[972] Howell and Potgieter (n 131), Pages 11-12.
[973] Ibid, Page 12.
[974] Ibid.

Currently, the most appropriate regulatory approaches regarding trades are: self-regulation for the peer-to-peer method, a licensing-system which necessitates the segregation of exchange-customer's assets for the exchange-based model, and a hybrid model of both of these approaches in line with the DEX method of transaction. There is sufficient public risk that is present within all three methods of transaction which justifies some degree of decentred regulatory intervention.[975] The above recommendations would be the most practical solutions towards increasing the legal protections for systematic errors within unpermissioned blockchain technology.

Although it has been recognised that the blockchain landscape is likely to evolve significantly over the coming years, reactive regulation would be problematic as it would leave users and markets exposed to the risks that are present. Consequently, there is a key recommendation for regulators to be pro-active in their regulatory approach and then adapt such an approach accordingly as the blockchain and regulatory landscapes continue to evolve. One key aspect could be the support and encouragement of permissioned blockchain platforms which if done successfully could attract users away from unpermissioned blockchain platforms. The main benefit of permissioned blockchain technology in this context is the legal protections available should any risks materialise, due to the centralised nature of the technology being more compatible with traditional legal frameworks.

The current regulatory approach within England with respect to liability for systematic errors within unpermissioned blockchain technology can be said to be limited, although as this thesis was in its final editing stages a consultation that might lead to a change of approach was announced. If further use of the technology continues, the risks associated will become more prominent. To mitigate against this, regulators may make a policy choice to move away from the current regulatory approach and

[975] Black (n 622), Pages 2-4; Black (n 151), Page 304.

towards one which provides greater legal protection for users within unpermissioned blockchain technology. Failure to do so could be highly problematic moving forward. The current FCA approach of warning users of the risks whilst providing minimal protection,[976] may be likely to be maintained providing market integrity and economic stability are not threatened.[977] However, in the recent consultation paper there is the recognition that as usage of the technology continues to increase, the regulatory approach must be flexible and adapt accordingly.[978] Global regulatory attention is growing in respect of liability issues within unpermissioned blockchain technology[979] and if England reaches the point where it feels necessary to take the next steps in governance of liability in this industry, then the recommendations provided in this chapter would be a key start.

[976] Chiu (n 100), Page 264.
[977] HM Treasury (n 120), Pages 8-11.
[978] Ibid, Pages 10-11.
[979] For further discussion of some of these developing and changing approaches see, Howell and Potgieter (n 131), Pages 9-11.

Chapter 7: Conclusion

Blockchain remains an evolving and fast developing topic. Case law is only just emerging, and regulation is in its infancy. Unpermissioned blockchain technology provides a unique technological development which presents unprecedented legal challenges. Although the extent to which such technology will be embraced is yet unclear, the potential of the technology is wide-reaching and could infiltrate many industries and become part of everyday life. This thesis has contributed to the discussion of the regulatory framework by examining the legal redress for systematic errors within unpermissioned blockchain technology.

This chapter will provide conclusions based on the preceding chapters. After a summary of the key findings from each of the prior six chapters there will be a conclusion and a direct answer to the key research questions from the thesis. There will then be discussion of the original contributions to knowledge from this thesis and a recognition of any limitations of the study. Finally, there will be some recommendations for future legal research that can be conducted in line with this thesis to further contribute to the field of knowledge within this area.

7.1: Key findings

Throughout the thesis, there has been a focus on unpermissioned blockchain technology and whether sufficient legal redress exists for systematic errors. It has been made clear that existing contractual and tort-based redress for fault has limitations within the unpermissioned blockchain context due to the approach to the law, the different methods of transaction, the decentralised nature of the technology[980] and the wide use by exchanges of contractual limitations on liability. The practicality of legal redress is further restricted due to the problems caused by the potential for anonymity

[980] Whereby there is a lack of clear organizational hierarchy see, Hong Kong Monetary Authority (n 66), Page 104.

within unpermissioned blockchain technology[981] and the jurisdictional issues that can arise with a supranational and decentred platform.[982] Blockchain technology does enable a degree of identification difficulty which provides a barrier to legal enforcement.[983] Although there is some debate as to whether true anonymity exists in unpermissioned blockchain technology, it can potentially undermine the legal protection for users. Anonymity may present difficulties if redress for those who suffer losses because of systematic errors is desired from a regulatory standpoint. In the future, legal clarity could be derived from a global convention and uniform legal approach across jurisdictions, but this is highly unlikely due to the differences in perception of the technology and variations in legal approaches,[984] legal procedure and further political differences between countries.[985]

For the peer-to-peer transactions, there will tend to be a lack of reliance on formal law that could provide a basis for liability, as well as an absence of the intention to be legally bound.[986] This renders the current legal framework as providing little to no form of redress regarding liability for systematic errors within the peer-to-peer model. Given the likely limitations as to the potential for law to provide an avenue for redress the thesis discussed whether liability issues could be resolved using Ostrom's self-

[981] Toshendra Kumar Sharma, 'How is blockchain verifiable by public and yet anonymous?' 10th July 2018 <https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/> Accessed 1st February 2023; Bodo, Gervais and Quintais (n 328), Page 312; Karl Wust and Aurthur Gervais, 'Do you Need a Blockchain?' (2018) Crypto Valley Conference on Blockchain Technology 45 <https://ieeexplore.ieee.org/document/8525392/authors> Accessed 1st February 2023, Page 45.

[982] Hari and Pasquier (n 184), Page 444 "When the anonymity of participants is concerned, complex questions arise in relation to applicable laws and competent jurisdictions."; Zetzsche, Buckley and Arner (n 141), Page 1392.

[983] Houben (n 60), Pages 263-264.

[984] For examples of how different jurisdictions react to Unpermissioned blockchain technology platforms such as Bitcoin in completely different manners, see Swan (n 212), Page 7. Additionally for a debate on how a cross-jurisdictional approach would apply to the issue of smart contracts, see Hari and Pasquier (n 184), Page 444.

[985] Hartley (n 295), Pages 6-8.

[986] Collyer Bristow (n 272), Minutes 32-34; Renwick and Gleasure (n 239), Page 30; *Hadley* v *Kemp* [1999] 4 WLUK 377, Page 623; *Blue* v *Ashley* [2017] EWHC 1928 (Comm), [2017] 7 WLUK 593, Para [56]; *Chitty on Contracts* (32nd edn, 2015) Vol 1, Paras 2-177, 2-194 and 2-195; *Tulip Trading Ltd* v *Bitcoin Association for BSV & Others* [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624, Para [67].

management theory as a possible self-regulatory model.[987] Although ultimately this approach was found to likely be impracticable. Within the peer-to-peer method, due to the intention of those involved, the coding can be regarded as paramount and so a regulatory approach that gives effect to this intention would be best-placed.[988] This approach also adheres to the idea that those who operate within the peer-to-peer method would potentially be able to find the most practical and informed solution to any fault that should arise.[989] It would be important to further understand whether there already exists an internal redress system if disputes should arise with some capability of sanctioning wrong-doing parties.[990]

Another key aspect that would be needed is the peer-to-peer method's "minimal recognition of rights to organise".[991] This means that whilst there needs to be freedom from external intervention, there must be enough legitimacy afforded from the state to individuals who seek to self-manage. Without state support it is difficult for the individuals to effectively govern. This can be in part due to the acceptance of state-based governance which can cause uncertainty surrounding the validity of self-governance, especially if there is no state support. Practically this could be the clarity from the regulators that the peer-to-peer method is not subject to legal intervention for systematic errors.

This thesis also assessed whether there is a broader need for regulation in view of public need. Predominantly, this need might arise at the point where the public's interaction with unpermissioned blockchain technology arises, most likely through the exchange-based cryptocurrency trading. During the assessment of the exchange-based

[987] Ostrom (n 618); Ostrom (n 791); For an interesting discussion on 'self-management' within decentralised platforms see, Chiu (n 100), Pages 295-297 and also pages 262, 280, 284 and 288.
[988] Yeung (n 254), Page 209; Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books 2006); Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999).
[989] Salmon and Myers (n 255), Page 4.
[990] Ostrom (n 618), Pages 94 and 100.
[991] Ibid, Page 101.

transactions in Chapter 6, it was noted that liability of the exchange is often limited through the terms and conditions of service and there is limited to no protection for the public in the event of loss through a fault within the underlying blockchain,[992] as opposed to fault on the part of the exchange. It may well be that such a risk may be viewed in a similar manner to other investment risks and is one that merely requires the public (specifically exchange customers) to be made aware of Julia Black's pluralistic regulatory approach.[993]

In Black's decentred approach, "regulation" is viewed as "the sustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour-modification."[994] This recognises the complexity of both society (with technological advancements such as unpermissioned blockchain technology) and the complexity of the law, which has numerous regulatory options which may be applied. Within such a view of regulation, the mere warning of risks, as hitherto adopted by UK financial regulators, can be accepted as a regulatory approach rather than only the command-and-control form of regulation. This approach of warning is commonly the policy choice of regulators that wish not to be active within speculative financial activity markets and do not want to be seen as instructing users what they should not do.[995] Providing the users are informed sufficiently, then theoretically such risk can be managed by the user themself instead of the state adopting a more paternalistic approach.[996]

[992] For an example, Binance state that to the maximum extent of the law they remove liabilities whether express or implied, so far as the law provides binance.com (n 203), Part IV Section 1.
[993] Currently it could be stated that users within this market are not aware of the risks see, Financial Conduct Authority (n 113), Page 12.
[994] Black (n 622), Page 26.
[995] Chiu (n 100), Page 264.
[996] Ibid. For further discussion of this, see section 6.1.

Regulation based on a lack of redress for fault in unpermissioned blockchains is not yet justified as the public risk from *liability issues* is relatively minimal, due largely to the current limited direct interaction of the public with unpermissioned blockchain technology. However, this does not automatically negate the debate of whether greater regulation of unpermissioned blockchain cryptocurrency is needed more generally. As the potential use of such technology increases, the potential for risk will increase likewise. The potential for further risk may be sufficient to warrant a developing regulatory framework which can evolve alongside the possible increased interaction with the technology.

In addition to this, the blockchain landscape continues to develop and the presence of DeFi exchanges (DEXs) as a vehicle for peer-to-peer transactions seemingly presents further diverse issues that may demand a hybrid regulatory approach between that of the peer-to-peer transactions and the traditional exchange-based transactions.[997]

7.2: Research Question Conclusion

The research question centres itself around two questions; firstly, is legal redress for systematic errors within unpermissioned blockchain technology possible, and secondly, would such legal redress be considered necessary. To effectively answer such questions, it is imperative that the different ways in which the general public may encounter unpermissioned blockchain technology should be recognised. Thus, it would be more appropriate to determine the possibility and necessity of legal redress for systematic errors within 1) peer-to-peer transactions, 2) exchange-based transactions and 3) the DEX method separately.

[997] Kruppa (n 93).

In answering the first question, legal redress for systematic errors within unpermissioned blockchain technology is unlikely. The decentralised,[998] supranational[999] technology that enables some level of anonymity[1000] does not seemingly conform to traditional models of contract or tort law in the UK. However, the identification of triable issues in the *Tulip Trading*[1001] case may lead to subsequent case law that clarifies this position. The answer to the second question is that a model of responsive regulation is desired,[1002] and some elements in the recent consultation paper appear to be moving in this direction.[1003] As the potential usage of unpermissioned blockchain technology increases, so will the level of risk in those markets and this may require further regulatory intervention moving forward.[1004]

Regulatory bodies such as the FCA have shown an ability to maintain regulatory oversight with money laundering regulations as an example, given the obvious risk of public harm if unpermissioned blockchains are used to facilitate the laundering of criminal proceeds or funds for terrorism. The threat of public harm from such activity can justify regulation following Black's risk-based justification, which states that governments have a responsibility to manage significant risks in society, which would include criminal activity.[1005] It is possible that such oversight could be developed from a liability perspective over the coming years only if self-regulation in the peer-to-peer method is not adequate[1006] and does not work sufficiently, giving rise to public harm, [1007] in accordance with Black's concept of risk as a justification for regulation within a

[998] Financial Conduct Authority (n 113), Page 23.
[999] Bjelajac and Bajac (n 54), Page 22.
[1000] Houben (n 60), Page 263.
[1001] *Tulip Trading* v *Van der Laan* [2023] EWCA Civ 83, [2023] 4 WLR 16, Paras [41] and [86].
[1002] Ayers and Braithwaite (n 656).
[1003] HM Treasury (n 120), Pages 8-11.
[1004] Howell and Potgieter (n 131), Page 1.
[1005] Black (n 151), Pages 303-309.
[1006] Within Ostrom's self-management theory, she recognises that such legitimisation is essential for the trust and development of the internal self-management framework itself. Ostrom (n 618), Page 101.
[1007] Howell and Potgieter (n 131), Page 1.

decentred view of regulation.[1008] The key point where the public may be most likely to experience risks within unpermissioned blockchain technology would be through the exchange-based method and the DEXs.[1009] The DEX method of transaction as a landscape is likely to become clearer and knowledge of this method is likely to increase in the future.[1010] The key aspect here is that by having more controls in the industry itself, the impact of risks could be mitigated.

In summary, whilst legal redress could be viewed as possible within the three methods of transactions discussed, the necessity of enhanced legal protection for systematic errors appears more complex of an issue. Within the peer-to-peer method of transaction there is the argument that peer-to-peer users will not expect recourse to law should any faults or errors occur on the blockchain. The exchange-based method and DEX method of transaction provide the possibility for a greater number of members of the public to become exposed to the risks presented by unregulated blockchain opportunities and this may be more of a regulatory concern. However, the main regulatory concern in this context is likely to be anti-money laundering, the prevention of scams and the prevention of misleading advertising impressions based on focusing only on winners who have made fortunes in cryptocurrency. The likelihood of further legal protection for systematic faults in the exchange-based and DEX methods of transaction is limited due to the lack of widespread interaction by the public. However, such markets are growing at a fast rate and the present level of risk is only likely to increase should interaction increase. Consequently, the threat of future risk within such markets seems to be the most compelling argument for necessity of enhanced legal protection within both the exchange-based and DEX methods of transaction.

[1008] Baldwin, Cave and Lodge (n 62), Page 3; Black (n 622), Page 11; Black (n 151), Pages 303-309.
[1009] Howell and Potgieter (n 131), Page 12.
[1010] Howell and Potgieter (n 131), Page 1; Johnstone (n 101), Page 169; Wilson and Westbrook (n 200), Page 1.

7.3: Thesis contributions

This thesis establishes the lack of legal redress through contract and tort in English law for systematic errors within unpermissioned blockchain technology. Furthermore, there is the determination that the current level of risk does not justify command-and-control regulation within the peer-to-peer method and that a decentred approach to regulation is more appropriate, including through self-regulation. Although Ostrom's self-management principles were considered as a possible model of self-regulation, they were found to be potentially problematic if used within the peer-to-peer method. This advances the knowledge within the field and provides a key work to be further analysed and critiqued.

More specifically the analysis throughout this thesis has provided three main contributions to knowledge. Firstly, by applying contract and tort law based on the English legal system to liability issues arising out of systematic errors within unpermissioned blockchain technology in the context of peer to peer transactions, it is clear that such avenues are likely to provide limited legal protection.[1011] Furthermore, any party who is seeking redress for loss suffered as a result of fault in an unpermissioned blockchain is likely to face significant practical difficulties, due to the decentralised nature of the technology and the potential anonymity of users and fraudsters.[1012] The second contribution to knowledge is the application of Ostrom's self-management theory to unpermissioned blockchain technology in the peer-to-peer context and the rejection of this approach as a possible governance solution.[1013] This can be distinguished from the work of Gazi and others,[1014] who focus on the changes

[1011] Application of contract and tort is difficult within the peer-to-peer method and liability is often limited in the exchange-based and DEX method.
[1012] For a brief discussion of how unpermissioned blockchain technology makes no reference to any hierarchy see, Hong Kong Monetary Authority (n 66), Page 104.
[1013] Ostrom (n 618); Ostrom (n 791); For an interesting discussion on 'self-management' within decentralised platforms see, Chiu (n 100), Pages 295-297 and also pages 262, 280, 284 and 288. For a discussion of Ostrom's self-management principle in blockchain and some problems that may occur see, Gazi and others (n 128).
[1014] Gazi and others (n 128).

that could be made to unpermissioned blockchain technology to conform to Ostrom's self-management theory,[1015] rather than the application of a truly decentralised platform to Ostrom's theory.

The third contribution to knowledge is provided with the recommendations for the regulatory landscape moving forward. By regulating within the decentred perspective,[1016] the broader regulatory approach is capable of more adequately dealing with the issues of the different methods of transaction as the potential risk within unpermissioned blockchain technology is not such that a command-and-control approach to regulation is presently merited.[1017] This negates the idea that unpermissioned blockchain technology is impossible to regulate but instead suggests that it may require a re-thinking of the regulatory landscape as we know it.[1018] Numerous policy choices exist for regulators[1019] which indicates that the current regulatory approach to liability within unpermissioned blockchain technology is not the only regulatory approach possible.[1020] Viewing regulation in a decentred manner[1021] and exploring some of the policy choices alluded to by Chiu[1022] would be a significant alteration from the current policy of the Financial Conduct Authority warning that risks exist, stating that there is limited legal protection,[1023] and attempting to control the some of the risks to the public through advertising.[1024] The latest consultation paper states that

[1015] Gazi and others (n 128), Pages 19-21.
[1016] Black (n 622), Pages 2-26.
[1017] Baldwin, Cave and Lodge (n 62), Page 3; Black (n 622), Page 11.
[1018] Chiu (n 100), Page 293.
[1019] Although it is worth mentioning that any policy choice would not necessarily prevent the use of an investment in such cryptocurrencies due to the presence of anonymity in the peer-to-peer model and the potential for 'regulatory arbitrage'. See, Chiu (n 100), Page 265.
[1020] Chiu (n 100), Pages 263-271.
[1021] Black (n 622), Pages 2-26.
[1022] Chiu (n 100), Pages 263-271.
[1023] Financial Conduct Authority (n 113), Page 12.
[1024] Financial Conduct Authority, 'Strengthening our financial promotion rules for high risk investments, including cryptoasset: Consultation Paper CP22/2' (FCA CP22/2 2022) <https://www.fca.org.uk/publication/consultation/cp22-2.pdf> Accessed 1st February 2023, Pages 46-51; Financial Conduct Authority, 'Strengthening our financial promotion rules for high-risk investments and firms approving financial promotions: Policy Statement PS22/10' (FCA PS22/10 2022) <https://www.fca.org.uk/publication/policy/ps22-10.pdf> Accessed 1st February 2023, Page 3.

changing from this policy will only happen if market integrity or macroeconomic stability are threatened, which the current usage level in the UK market suggests would be unlikely.[1025] As the usage level remains low, so does the risk, however, the risk of impact to the public will increase as usage increases. The UK government have acknowledged this in the recent consultation paper by indicating an intent to provide an agile approach to regulatory intervention for such risks.[1026] Therefore the current approach is likely to remain at present,[1027] however, the regulatory landscape may evolve as the interaction with the technology develops.[1028] This thesis proposes that the main focus for regulation should be at the point where the public are exposed to unpermissioned blockchain technology, namely through cryptocurrency exchanges. Problems with exchanges can be dealt with through contract law but it is the recommendation that a licensing system is developed in-line with the current requirement of registration.[1029]

In summary, the key contributions of this thesis suggest that regulatory attention must be paid to the risk of systematic errors within unpermissioned blockchain technology and the potential liability issues that could arise. Moving forward, this thesis can provide insight into the types of risks that are present, current potential for redress in contract and tort, the importance of distinguishing between different forms of blockchain and their methods of transaction, and the recommended regulatory

[1025] HM Treasury (n 120), Pages 8-11.
[1026] Ibid, Pages 10-11.
[1027] Chiu (n 100), Page 264.
[1028] For example, there is the possibility for *Lex Cryptographia* to be further developed. For further insight into this see, Wright and De Filippi (n 616); Johnstone (n 101), Pages 260-261; Michael Schillig, 'Lex Cryptographi(c)a, Cloud Crypto Land or What? – Blockchain Technology on the Legal Hype Cycle' (2023) 86(1) Modern Law Review 31, Page 42; Thibault Schrepel, 'Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia' (2019) in *General Principles and Digitalisation* (Hart Publishing, 2020), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3485436> Accessed 1st February 2023, Page 373. Additionally, a licensing system for exchanges or a list of trusted cryptocurrencies could be alternative approaches that could be implemented. For a discussion of the similarities between cryptocurrency and gambling and the presence of a licensing system in the gambling industry see, Paul Delfrabbro and others, 'Cryptocurrency trading, gambling and problem gambling' (2021) 122 Addictive Behaviours 1, Pages 1-2; gamblingcommission.gov, 'home' <https://www.gamblingcommission.gov.uk/> Accessed 1st February 2023.
[1029] For more information on such a registration requirement, see Financial Conduct Authority (n 511).

approaches[1030] that should be taken now to provide a clear framework which can be flexible to the evolution[1031] that is coming.[1032]

7.4: Limitations of the study

It is recognised that there are some limitations within this thesis. Three limitations will be raised. Firstly, it is recognised that the topic of unpermissioned blockchain technology is a broad subject area. It is a fast-moving technology and a topic of academic debate that is still developing, with the *Tulip Trading* case law only emerging towards the end of the project. The main consequence of this is that some discussions within unpermissioned blockchain technology were beyond the scope of this thesis but would be relevant for how the law will interact with unpermissioned blockchain technology. For example, further analysis of smart contracts,[1033] the Ethereum blockchain, and DAOs as a way of collective decision making,[1034] all of which were only touched upon, and liability issues within NFTs[1035] were all beyond the scope of this thesis but remain topics for academic debate moving forward.

[1030] For further discussion of some of these developing and changing approaches see, Howell and Potgieter (n 131), Pages 9-11.

[1031] For some examples of how the landscape may change in coming years see, Andreas Bogner, Mathieu Chanson and Arne Meeuw, 'A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain' IoT'16: Proceedings of the 6th International Conference on the Internet of Things (November 2016) 177 <https://doi.org/10.1145/2991561.2998465> Accessed 1st February 2023; Foteni Valeonti and others, 'Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs)' (2021) 11 Applied Sciences 9931 <https://www.mdpi.com/2076-3417/11/21/9931#cite> Accessed 1st February 2023; Maria Demertzis, 'Non-fungible tokens (NFTs): The next chapter in crypto' (January 2022) Bruegel-Blogs <https://go.gale.com/ps/i.do?id=GALE%7CA690531927&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=&p=AONE&sw=w&userGroupName=anon%7Ed2a2fd82> Accessed 1st February 2023; The Truth Drops (n 969).

[1032] Howell and Potgieter (n 131), Pages 11-12.

[1033] Andreas Bogner, Mathieu Chanson and Arne Meeuw, 'A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain' IoT'16: Proceedings of the 6th International Conference on the Internet of Things (November 2016) 177 <https://doi.org/10.1145/2991561.2998465> Accessed 1st February 2023.

[1034] For further discussion of DAO governance see, Mondoh and others (n 948). For further discussion of rules of liability being coded into this see, Peder Ostbye, 'Exploring DAO Members' Individual Liability' (February 2022) Discussion paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4045799> Accessed 1st February 2023.

[1035] Foteni Valeonti and others, 'Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs)' (2021) 11 Applied Sciences 9931 <https://www.mdpi.com/2076-3417/11/21/9931#cite> Accessed 1st February 2023; Maria Demertzis, 'Non-fungible tokens (NFTs): The next chapter in crypto' (January 2022) Bruegel-Blogs <https://go.gale.com/ps/i.do?id=GALE%7CA690531927&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=&p=AONE&sw=w&userGroupName=anon%7Ed2a2fd82> Accessed 1st February 2023.

The second limitation of this study is the lack of insight from insiders of unpermissioned blockchain technology. The conducting of interviews and a sociological study of attitudes among coders and miners and approaches to dispute resolution was beyond the scope of this project but is a worthy subject for future study.

The third and final limitation is derived from the fact that a more holistic study of unpermissioned blockchain technology would require an interdisciplinary approach. For example, an analysis of the construction of coding and whether that impacts liability or whether it could be possible that there would be an internal redress system embedded into the code of a platform and how that may operate would have enhanced this project further.[1036]

7.5: Recommendations for future research

This thesis advances knowledge within the academic area, but it also signifies additional topics of research which would further benefit the academic debate. This section will highlight the key topics that require research and that would build not only on this thesis but the body of academic works. Firstly, further research is required for the topic of DEXs. This is an area recognised as requiring more regulatory attention and the same could be said from an academic perspective.[1037] It will be important to better understand their intricate operations and whether there is some degree of standardised practice amongst DEXs. Similar to the discussion in this thesis whereby the risks of exchanges were highlighted and a need for greater regulation was suggested. Secondly, further discussion is needed in respect of an inter-disciplinary analysis of the internal rules and underlying coding with its legal implications. This would provide an informed

[1036] This is also based on the discussion of 'code as law' but would be enhanced with a deeper analysis of the code itself. For further discussion of 'code as law' see, Yeung (n 254), Page 209; Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books 2006); Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999).
[1037] Kruppa (n 93).

analysis which will increase understanding of the technical components of the peer-to-peer method of transaction and how that should translate into legal frameworks.

The third recommended research to be conducted moving forward is an empirical analysis to better understand the perspectives of the peer-to-peer users in the peer-to-peer method and the exchange customers in the exchange-based method and DEX method. This was recognised as a limitation of this study but the sociological study of attitudes among users would warrant its own thesis of discussion which was beyond the scope of this project. The FCA have acknowledged that users within the cryptocurrency sphere are unaware of the risks that are present,[1038] however, research is needed to better understand the expectations of these users with regards to how risk or disputes are likely to be dealt with in such methods of transaction as well as their understanding of the technology itself. Such research would better inform policy makers as to whether there is an expectation of legal intervention or some degree of consent of the risks present which would in-turn influence the need for regulatory intervention. This could also be used to indicate whether such awareness of risks has changed since the FCA made such a statement in 2019.

The fourth topic of recommended research centres around the additional potential risks in peer-to-peer transactions. It has been acknowledged that such threats have not seemingly widely manifested, however, it would be beneficial to further research how likely these potential threats are. For example, more detailed analysis into mining pools would be valuable from an academic and regulatory perspective. This would involve an assessment of the environmental impact of mining pools and the potential for the 51% hack.[1039] The potential for the latter is growing, given the increasing concentration of mining in the hands of a decreasing pool of miners.[1040] Other issues such as

[1038] Financial Conduct Authority (n 113), Page 12.
[1039] Dirk Zetzsche Et Al, The Distributed Liability of Distributed Ledgers: Legal risks of Blockchain (2018) University of Illinois Law Review 1361, Pages 1378-1380; Nakamoto (n 51), 1.0 Introduction.
[1040] This may be a trend that is likely to continue given the rising energy prices also.

cryptographic key theft and any errors in the coding of unpermissioned blockchain technology would also provide valuable insight.[1041]

Furthermore, and linked to this thesis, the fifth recommended research would be a thorough investigation of the terms and conditions of all cryptocurrency exchanges in the UK, or another specific jurisdiction would provide a more in-depth analysis of the industry practices and the extent to which liability is restricted, as well as potential jurisdictional complexities that may be raised for the enforcement of claims. Building upon this there might be an inter-disciplinary investigation where the asset-handling practices of the exchanges were monitored to better understand the way client assets and information is stored and secured. The scope of such research could be extended to analyse fiduciary duties in relation to exchanges for example.[1042]

Finally, the last recommended research would be the exploration of data protection issues and laws in the context of unpermissioned blockchain technology.[1043] This would involve a more thorough analysis of whether true anonymity exists in unpermissioned blockchain technology and if a system stores any personal information, who would data protection laws be applied to in a decentralised system.

Whilst these provide a small range of topics to be analysed moving forward, it is recognised that not only will the blockchain and regulatory landscape evolve significantly over the coming years,[1044] the same will also likely be true for the

[1041] For more information on cryptographic key theft see ID-3, 'Cryptographic Key Management – the Risks and Mitigation' 29th April 2019 <https://id-3.co.uk/cryptographic-key-management-the-risks-and-mitigation/>Accessed 1st February 2023. For further information on the threat of wallet theft see, UK Government Chief Scientific Adviser (n 237), Page 12.
[1042] Haque and others (n 439), Page 186.
[1043] Finck (n 156).
[1044] For further discussion of how the regulatory landscape may change see, Howell and Potgieter (n 131), Pages 9-11. For some examples of how the blockchain landscape may change in coming years see, Bogner, Chanson and Meeuw (n 1033); Foteni Valeonti and others, 'Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs)' (2021) 11 Applied Sciences 9931 <https://www.mdpi.com/2076-3417/11/21/9931#cite> Accessed 1st February 2023; Maria Demertzis, 'Non-fungible tokens (NFTs): The next chapter in crypto' (January 2022) Bruegel-Blogs <https://go.gale.com/ps/i.do?id=GALE%7CA690531927&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=&p=AONE&sw=w&userGroupName=anon%7Ed2a2fd82> Accessed 1st February 2023; The Truth Drops (n 969).

academic landscape. Further research will be necessary for this novel technology which has potential to permeate many aspects of daily life.

Bibliography

UK Legislation

Companies Act 2006

Consumer Protection Act 1987

Consumer Rights Act 2015 c15

Data Protection Act 2018 (c.12)

Financial Services and Markets Act 2000

Financial Services and Markets Bill, (HL Bill 80) <https://bills.parliament.uk/publications/49063/documents/2625> Accessed 1st February 2023

Gambling Act 2005

Sale of Goods Act 1979

International Legislation

Directive 95/46/EC

EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Treaty on the Functioning of the European Union (TFEU)

Uniform Customs and Practice for Documentary Credits (2007 revision, ICC Publication no. 600) (UCP600)

UK Cases

AA v Persons Unknown & Others [2019] EWHC 3556 (Comm), [2020] 4 WLR 35

Balfour v Balfour [1919] 2 KB 571

Shamil Bank of Bahrain EC v Beximco Pharmaceutical Ltd [2004] EWCA Civ 19, [2004] 1 WLR 1784

Blue v Ashley [2017] EWHC 1928 (Comm), [2017] 7 WLUK 593

Bolton v Stone [1951] AC 850

Caparo Industries Plc v Dickman [1990] 2 AC 605

Customs & Excise Commissioners v Barclays Bank plc [2006] UKHL 28, [2007] 1 AC 181

Dubai Aluminium Co Ltd v Salaam [2002] UKHL 48, [2003] 2 AC 366

Esso Petroleum Co v Customs and Excise Commissioners [1976] 1 WLR 1

Fetch.ai Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm), [2021] WLUK 601

First Energy (UK) Ltd v Hungarian International Bank Ltd [1993] 2 Lloyd's Rep 194

Fitzgerald v Lane [1987] QB 781

Hadley v Kemp [1999] 4 WLUK 377

Halpern v Halpern [2007] EWCA Civ 291, [2008] QB 195

Hamid v Francis Bradshaw Partnership [2013] EWCA Civ 470, [2013] 5 WLUK 69

Ion Science Ltd v Persons Unknown and Others (unreported) 21st December 2020 (Commercial Court)

Latimer v AEC Ltd [1953] AC 643

Modahl v British Athletic Federation [2001] EWCA Civ 1447, [2002] 1 WLR 1192

National Carriers Ltd v Panalpina (Northern) Ltd [1981] AC 675

Nettleship v Weston [1971] 2 QB 691

Prest v Petrodel Resources Limited and others [2013] 3UKSC 34, [2013] 2 AC 415

Ramona Ang v Reliantco Investments Ltd [2020] EWHC 3242 (Comm), [2020] 11 WLUK 428

Robinson (Appellant) v Chief Constable of West Yorkshire Police (Respondent) [2018] UKSC 4, [2018] AC 736

Salomon v A Salomon & Co Ltd [1897] AC 22

Singularis Holdings Ltd (In Official Liquidation) (A Company Incorporated in the Cayman Islands) (Respondent) v Daiwa Capital Markets Europe Ltd (Appellant) [2019] UKSC 50, [2020] AC 1189

Smith v Littlewoods [1987] AC 241

Spartan Steel & Alloys Ltd v Martin & Co (Contractors) Ltd [1973] QB 27

Storer v Manchester City Council [1974] 1 WLR 1403

Tulip Trading Ltd v Bitcoin Association for BSV & Others [2022] EWHC 667 (Ch), [2022] 2 All ER (Comm) 624

Tulip Trading v Van der Laan [2023] EWCA Civ 83, [2023] 4 WLR 16

Vaughan v Menlove (1837) 132 ER 490

Wang v Darby [2021] EWHC 3054 (Comm), [2022] Bus LR 121

Ward v London County Council [1938] 2 All ER 341

Watt v Hertfordshire County Council [1954] 1 WLR 835

International Cases

Berk v Coinbase 840 Fed Appx 914, (9th Cir, 23rd December 2020) (not for publication) rev'g 2019 WL 3561926 (ND Calif 6th August 2019)

BMA LLC v HDR Global Trading Ltd 2021 WL 949371 (ND Calif 12th March 2021)

In re Tezos Securities Litigation, No. 17-CV-06779-RS (N.D.Cal. Aug. 7, 2018)

Shin v ICON Found 2021 WL 1893117 (ND Calif 11th May 2021)

United States of America before the Securities and Exchange commission In the Matter of Zachary Coburn, Release No 84553, File No 3-18888 (8th November 2018) <https://www.sec.gov/files/litigation/admin/2018/34-84553.pdf> Accessed 1st August 2023

Official Materials

Bank of England Financial Policy Committee, 'Financial Policy Committee Statement from its policy meeting 12 March 2018' (FPC 2018) <https://www.bankofengland.co.uk/-/media/boe/files/statement/fpc/2018/financial-policy-committee-statement-march-2018.pdf?la=en&hash=61059A79F4453B2EFA6BA88A598739DD67FC0CD7> Accessed 1st February 2023

Bank of England, 'Digital Currencies' (5th March 2019) <https://www.bankofengland.co.uk/research/digital-currencies> Accessed 1st February 2023

Dr Michèle Finck (STOA), 'Blockchain and the General Data Protection Regulation' (2019) PE 643.445 July, <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> Accessed 1st February 2023

Financial Conduct Authority, 'Cryptoassets: Ownership and attitudes in the UK' (FCA March 2019) <https://www.fca.org.uk/publication/research/cryptoassets-ownership-attitudes-uk-consumer-survey-research-report.pdf> Accessed 1st February 2023

Financial Conduct Authority, 'Cryptoassets' (2019) <https://www.fca.org.uk/consumers/cryptoassets> Accessed 1st February 2023

Financial Conduct Authority, 'Do I need to register with the FCA for carrying on cryptoasset activity?' (2019) <https://www.fca.org.uk/publication/documents/cryptoasset-registration-flowchart.pdf> Accessed 1st February 2023

Financial Conduct Authority, 'DP17/3: Discussion Paper on distributed ledger technology' (FCA DP17/3 2017) <https://www.fca.org.uk/publication/discussion/dp17-03.pdf> Accessed 1st February 2023

Financial Conduct Authority, ‘FCA warns consumers of the risks of investments advertising high returns based on cryptoassets’ (January 2021) <https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets> Accessed 1st February 2023

Financial Conduct Authority, ‘Guidance on Cryptoassets: Consultation Paper CP19/3’ (FCA CP19/3 2019) <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> Accessed 1st February 2023

Financial Conduct Authority, ‘How and why consumers buy cryptoassets: a report for the FCA’ (FCA October 2018) <https://www.fca.org.uk/publication/research/how-and-why-consumers-buy-cryptoassets.pdf> Accessed 1st February 2023

Financial Conduct Authority, ‘PS19/4: Asset Management Market Study - further remedies’’ (FCA PS19/4 2019) <https://www.fca.org.uk/publication/policy/ps19-04.pdf> Accessed 1st February 2023

Financial Conduct Authority, ‘Register Cryptoasset firms’ <https://register.fca.org.uk/s/search?predefined=CA> Accessed 1st February 2023

Financial Conduct Authority, ‘Strengthening our financial promotion rules for high risk investments, including cryptoasset: Consultation Paper CP22/2’ (FCA CP22/2 2022) <https://www.fca.org.uk/publication/consultation/cp22-2.pdf> Accessed 1st February 2023

Financial Conduct Authority, ‘Strengthening our financial promotion rules for high-risk investments and firms approving financial promotions: Policy Statement PS22/10’ (FCA PS22/10 2022) <https://www.fca.org.uk/publication/policy/ps22-10.pdf> Accessed 1st February 2023

Financial Conduct Authority, ‘The Listing Rules’ (January 2023) <https://www.handbook.fca.org.uk/handbook/LR.pdf> Accessed 1st February 2023

Financial Conduct Authority, ‘Unregistered Cryptoasset Businesses’ (February 2022) <https://register.fca.org.uk/s/search?predefined=U> Accessed 1st February 2023

Gambling Commission, ‘Home’ <https://www.gamblingcommission.gov.uk/> Accessed 1st February 2023

Gensler G, ‘Prepared Remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference’ (April 2022) <https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422> Accessed 1st February 2023

Government Office for Science (2008). *Distributed Ledger Technology: beyond block chain,* <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 1st February 2023

Government Office for Science (2015), *Distributed Ledger Technology: beyond block chain*, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 1st February 2023

HM Land Registry, 'HM Land Registry to explore the benefits of blockchain' (2018) <https://www.gov.uk/government/news/hm-land-registry-to-explore-the-benefits-of-blockchain> Accessed 1st February 2023

HM Treasury, 'Future financial services regulatory regime for cryptoasset: Consultation and call for evidence' (February 2023) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf> Accessed 1st February 2023

HM Treasury, 'Government sets out plan to make UK a global cryptoasset technology hub' (April 2022) <https://www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub> Accessed 1st February 2023

HM Treasury, 'The digital Pound: a new form of money for households and businesses?' (CP797, February 2023) <https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper> Accessed 7th February 2023

Hong Kong Monetary Authority, 'Whitepaper On Distributed Ledger Technology 1.0' (HKMA 2016) <https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf> Accessed 1st February 2023

Hong Kong Monetary Authority, 'Whitepaper On Distributed Ledger Technology 2.0' (HKMA 2017) <https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20171025e1a1.pdf> Accessed 1st February 2023

House of Lords Paper (Select Committee on Communications), Regulating in a digital world, 2nd report of Session 2017-2019 (March 2019), HL Paper 229

Law Commission, *Smart Legal Contracts Advice to Government* (Law Com No 401, 2021)

Raab D, Ministry of Justice, 'Improving UK Competitiveness, Strengthening the Rule of Law' (Speech at the Policy Exchange, London, 7th December 2017) <https://www.gov.uk/government/speeches/improving-uk-competitiveness-strengthening-the-rule-of-law> Accessed 1st February 2023

UK Government Chief Scientific Adviser – Mark Walport (Government Office for Science), 'Distributed Ledger Technology: beyond block chain (GS/16/1) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> Accessed 1st February 2023

UK Jurisdiction Taskforce, 'Legal statement on cryptoassets and smart contracts' (The LawTech Delivery Panel) <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.lawgazette.co.uk%2Fcommentary-and-opinion%2Fcrypto-law-still-has-known-unknowns%2F5102223.article&data=01%7C01%7Caki.elmenshawy2014%40my.ntu.ac.uk%7Cefb8a9bf0b174b638aa508d76e9e77dc%7C8acbc2c5c8ed42c78169ba438a0dbe2f%7C0&sdata=vHbPiEGhadPlL6gWdBSgBhGOHE3uBavzGk%2BN4i%2B1xwQ%3D&reserved=0> Accessed 1st February 2023

UK Jurisdiction Taskforce, 'The Launch of the Legal Statement on the Statues of Cryptoassets and Smart Contracts' (November 2019) <https://www.judiciary.uk/wp-content/uploads/2019/11/LegalStatementLaunch.GV_.2-1.pdf > Accessed 1st February 2023

World Anti-Doping Code (2015 with 2019 amendments) <https://www.wada-ama.org/sites/default/files/resources/files/wada_anti-doping_code_2019_english_final_revised_v1_linked.pdf> Accessed 1st February 2023

Books

Abaunza D A, *The Law for Energy Prosumers* (Springer 2022)

Ayers I and Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992)

Ayres I and Braithwaite J, 'Responsive Regulation: Transcending the Deregulation Debate', in Martin Lodge, Edward Page and Steven Balla (eds), *The Oxford Handbook of Classics in Public Policy and Administration* (Oxford University Press 2015)

Baldwin R, Cave M and Lodge M, *Understanding regulation: theory, strategy, and practice* (2nd edn, Oxford University Press 2012)

Barnett R E, 'Rights and remedies in a consent theory of contract' in Gillespie Frey R and Morris C (eds) *Liability and responsibility: essays in law and morals* (Cambridge University Press 1991)

Bharti S, *Corporate Social Responsibility in India* (Palgrave Macmillan 2022)

Black J, 'The Role of Risk in Regulatory Processes' in Baldwin R, Cave M and Lodge M (ed), The Oxford Handbook of Regulation (Oxford University Press 2010)

Blind K, 'The Impact of Regulation on Innovation' in Edler J and others (eds), *Handbook of Innovation Policy Impact* (Elgar Publishing 2016)

Cahillane L and Schweppe J, *Legal Research Methods: Principles and Practicalities* (Clarus Press 2016)

Campbell Black H, *Black's Law Dictionary* (2nd edn Lawbook Exchange 1995)

Campbell-Verduyn M, *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018)

Chitty on Contracts (32nd edn, 2015) Vol 1

Chiu I, *Regulating the Crypto Economy Business Transformations and Financialisation* (Hart Publishing 2021)

Coleman J, Hershovitz S and Mendlow G, 'Theories of the Common Law of Torts' in Zalta E N (ed) *The Stanford Encyclopedia of Philosophy, substantive revision* (Winter 2015) <https://plato.stanford.edu/entries/tort-theories/> Accessed 1st February 2023

De Filippi P and Wright A, *Blockchain and the Law: The Rule of Code* (Harvard University Press, 2018)

Epstein R, 'Beyond foreseeability: consequential damages in the law of contract' in Gillespie Frey R and Morris C (eds) *Liability and responsibility: essays in law and morals* (Cambridge University Press 1991)

Ezra P J and others, 'Secured Communication Using Virtual Private Network (VPN)' in Khanna K, Vieira Estrela V and Coelho Rodrigues J J P (ed), *Cyber Security and Digital Forensics: Lecture Notes on Data Engineering and Communications Technologies 71* (Springer, Singapore 2021)

Fleming J G, *The Law of Torts* (9th edn, North Ryda, NSW: LBC Information Services 1998)

Fried C, *Contract as Promise: A Theory of Contractual Obligation* (Oxford University Press 2015, 2nd edn)

Frisby D, *Bitcoin: The Future of Money?* (Unbound 2014)

Ghosh S, 'Blockchain and Beyond' in Chishti S, Craddock T and Courtneidge R (ed) *The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries* (Wiley 2019)

Goldbach R, *Global Governance and Regulatory Failure: The Political Economy of Banking* (Palgrave Macmillan 2015)

Hall K, *The Oxford Companion to American Law* (Oxford University Press 2002)

Hancher L and Moran M, *Organizing regulatory space* (1989) as found in Baldwin R, Scott C and Hood C, *A reader on Regulation* (Oxford University Press 1998)

Hinkelman E, *A short course in International payments: how to use letters of credit, D/P and D/A terms, prepayment, credit, and cyberpayments in international transactions*, (2nd edn, World Trade Press 2009)

Hutchinson T, 'Chapter 1: Doctrinal Research' in Watkins D and Burton M (ed), *Research Methods in Law* (2nd edn, Routledge 2017)

Johnstone S, *Rethinking the Regulation of Cryptoassets: Cryptographic Consensus Technology and the New Prospect* (Elgar Publishing 2021)

Kimel D, *From Promise to Contract: Towards a Liberal Theory of Contract* (Bloomsbury 2003)

Law J and Martin E, *A Dictionary of Law* (Oxford University Press 2009, 7th edn)

Lessig L, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999)

Lessig L, *Code: Version 2.0* (New York: Basic Books 2006)

Lothian T, *Law and the Wealth of Nations* (New York: Columbia University Press 2016)

McConville M and Chui W H, Research Methods for Law (2nd edn, Edinburgh University Press 2017)

McEntire J and Kennedy A, *Food Traceability* (Springer 2019)

Morgan B and Yeung K, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, 2007)

Offe C, *Contradictions of the Welfare State* (Routledge 1984)

Ogus A, *Regulation: Legal Form and Economic Theory* (Clarendon Press 1994),

Ostrom E, 'Tragedy of the Commons', in Steven N Durlauf and Lawrence E Blume (ed) *The New Palgrave Dictionary of Economics* (2nd edn Palgrave Macmillan 2008)

Ostrom E, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press 1990)

Paul R and others (eds), *Society, Regulation and Governance: New Modes of Shaping Social Change?* (Edward Elgar Publishing 2017)

Pitel S and Rafferty N, *Conflict of Laws* (Irwin Law Inc, 2016, 2nd ed)

Schrepel T, 'Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia' (2019) in *General Principles and Digitalisation* (Hart Publishing, 2020), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3485436> Accessed 1st February 2023

Storublevtcev N, 'Cryptography in Blockchain' in Misra S and others (eds) *Computational Science and Its Applications – ICCSA* (Springer Nature 2019)

Swan M, *Blockchain: Blueprint for a New Economy* (O'Reilly 2015)

Tasca P and Piselli R, *The Blockchain Paradox* (Oxford University Press, 2019)

Teubner G ed, *Juridification of Social Spheres: A Comparative Analysis of Labor, Corporate, Antitrust and Social Welfare Law* (Walter de Gruyter 2012)

Trevor Hartley, *International commercial litigation: text, cases and materials on private international law* (Cambridge University Press, 2nd edn, 2015)

Van Hoeke M, *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Bloomsbury 2011)

Walch A, 'In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains' in Lianos I, Hacker P, Eich S and Dimitropoulos G (ed) *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019)

Xiwei Xu, Ingo Weber and Mark Staples, *Architecture for Blockchain Applications* (Springer 2019)

Zhen Zheng, *The Legal System of Art Auction in China* (Springer 2022)

Dictionaries

Cambridge Dictionary, 'Cryptocurrency' (2023) <https://dictionary.cambridge.org/dictionary/english/cryptocurrency>Accessed 1st February 2023

Cambridge Dictionary, 'Immutable' (2023) <https://dictionary.cambridge.org/dictionary/english/immutable> Accessed 1st February 2023

Cambridge Dictionary, 'Ledger' (2020) <https://dictionary.cambridge.org/dictionary/english/ledger> Accessed 1st February 2023

Cambridge dictionary, 'Pseudonymous' (2023) <https://dictionary.cambridge.org/dictionary/english/pseudonymous> Accessed 1st February 2023

encyclopedia.com, 'Cryptography, Public and Private Key' 16th March 2020 <https://www.encyclopedia.com/economics/encyclopedias-almanacs-transcripts-and-maps/cryptography-public-and-private-key> Accessed 1st February 2023

Merriam-Webster Online dictionary, 'lex domicilii' <https://www.merriam-webster.com/dictionary/lex%20domicilii> Accessed 1st February 2023

Journal Articles

Agarwal R, Thapliyal T and Shukla S, 'Analyzing Malicious Activities and Detecting Adversarial Behaviour in Cryptocurrency based Permissionless Blockchains: An Ethereum Usecase' (2022) 1(2) Distributed Ledger Technologies: Research and Practice, Article 8

Agnikhotram S and Kouroutakis A, 'Doctrinal Challenges for the Legality of Smart Contracts: Lex Cryptographia or a New, Smart Way to Contract' (2019) 19 Journal of High Technology Law 300

Agrell P J, 'Incentive Regulation of Networks: Concepts, definitions and models' (2015) 1(2) Reflets et Perspectives de la vie Economique 103

Al-Adwan Dr M K M, 'The legitimacy of Online Alternative Dispute Resolution (ODR)' (2011) 2(19) International Journal of Business and Social Science 167

Allen HJ, 'Driverless Finance' (2020) 10 Harvard Business Law Review 157

Araral E, 'Ostrom, Hardin and the commons: A critical appreciation and a revisionist view' (2014) 36 Environmental Science & Policy 11

Atzori M, 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' (2017) 6(1) Journal of Governance and Regulation 45

Babich V and Hilary G, ‘Blockchain and other Distributed Ledger Technologies in Operations’ (2019) 12(2-3) Foundations and Trends in Technology, Information and Operations Management 152

Babich V and Hilary G, ‘OM Forum – Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology’ (2019) 22(2) Manufacturing & Service Operations Management 223

Badea L and Mungiu-Pupazan M C, ‘The Economic and Environmental Impact of Bitcoin’ (2021) 9 IEEE 48091

Beale H and Dugdale T, ‘Contracts between Businessmen: Planning and the Use of Contractual Remedies’ (1975) 2 Brit JL & Soc’y 45

Becker K, ‘Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries’ (2022) 33 Law Critique 113

Bennet Marrow P, Karol M and Kuyan S, ‘Artificial Intelligence and Arbitration: The Computer as an Arbitrator – Are We There Yet?’ (2020) 74(4) Dispute Resolution Journal 35

Bhaskari D L and Sri P S G A, ‘A study on blockchain technology’ (2018) 7 (2.7) International Journal of Engineering & Technology 418

Bjelajac Z and Bajac M, ‘Blockchain Technology and Money Laundering’ (2022) 39(2) Pravo-Teorija I Praska 21

Black J, ‘Critical Reflections on Regulation’ (2002) 27 Australian Journal of Legal Philosophy 1

Balasubramanian S and others, ‘A readiness assessment framework for Blockchain adoption: A healthcare case study’ (2021) 165 Technological Forecasting and Social Change

Block W and Jankovic I, ‘Tragedy of the Partnership: A Critique of Elinor Ostrom’ (2016) 75(2) American Journal of Economics and Sociology 289

Bodo B, Gervais D and Quintais J P, ‘Blockchain and smart contracts: the missing link in copyright licensing?’ (2018) 26 (4) International Journal of Law and Information Technology 311

Bolognini L and Bistolfi C, ‘Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation’ (2017) 33 Computer Law & Security Review 171

Broadbent J, Dietrich M and Laughlin R, ‘The Development of Principal-Agent, Contracting and Accountability Relationships in the Public Sector: Conceptual and Cultural Problems’ (1996) 7(3) Critical Perspectives on Accounting 259

Buck Cox S J, ‘No Tragedy of the Commons’ (1985) 7(1) Environmental Ethics 49

Caliskan K, ‘The Elephant in the Dark: A New Framework for Cryptocurrency Taxation and Exchange Platform Regulation in the US’ (2022) 15(3) Journal of Risk and Financial Management 118

Cate F and others, ‘Blockchain versus data-protection’ (2018) 8(2) International Data Privacy Law 103

Cohen G, ‘The fault that lies within our Contract Law’ (2008) 107 Michigan Law Review 1445

Cole D, ‘When is Command-and-Control Efficient? Institutions, Technology, and the Comparative Efficiency of Alternative Regulatory Regimes For Environmental Protection’ (1999) Wisconsin Law Review 887

Coleman J, ‘Corrective Justice and Wrongful Gain’ (1982) 11 J Legal Stud 421

Connolly B (Flynn O’Driscoll), ‘Cybersecurity breaches: the risks and how to mitigate them’ (2017) 6(1) Compliance & Risk 7

Cooter R, ‘Economic Theories of Legal Liability’ (1991) The Journal of Economic Perspectives 5 (3) 11

Copestake A, Furceri D and Gonzalez-Dominguez P, ‘Crypto market responses to digital asset policies’ (2023) Economic Letters 222, Article 110949

Daintith T, ‘A Regulatory Space Agency’ (1989) 9(4) Oxford Journal of Legal Studies 534

Davis M, ‘Necessity and Nozick’s Theory of Entitlement’ (1977) 5(2) Political Theory 219

De Filippi P and Loveluck B, ‘The indivisible politics of Bitcoin: governance crisis of a decentralised infrastructure’ (2016) 5(4) Internet Policy Review 1

de Vries A, ‘Bitcoin boom: What rising prices mean for the network’s energy consumption’ (2021) 5(3) Joule 509

Delfabbro P and others, ‘Cryptocurrency trading, gambling and problem gambling’ (2021) 122 Addictive Behaviours 1

Djurovic M and Janssen A, ‘The Formation of Blockchain-based Smart Contracts in the Light of Contract Law’ (2018) 26(6) European Review of Private Law 753

Dogan S and Lemley M, ‘Antitrust Law and Regulatory Gaming’ (2009) 87 Texas Law Review 685

Domingos Taufik R, ‘Block Change: The Fallacy of Blockchain Immutability and Cartel Governance’ (2020) 1 Notre Dame Journal on Emerging technologies 307

Dudgeon N and Malna G, ‘Distributed Ledger Technology: From Blockchain to ICOs’ (2018) 37(2) Banking & Financial Services Policy Report 4

Edelstein J, ‘Anonymity and international law Enforcement in Cyberspace’ (1996) Autumn (1) Fordham Intellectual Property, Media & Entertainment Law Journal 231

Egbuonu K, ‘Norwich Pharmacal orders: business interests and exemplary conduct can be relevant’ (2014) 9(11) Journal of Intellectual Property Law & Practice 882

Evans T, ‘Role of International Rules in Blockchain-Based Cross-Border Commercial Disputes’ (2019) 65 Wayne Law Review 1

Feinberg J, ‘Voluntary Euthanasia and the Right to Life’ (1978) 7 Phil Pub Aff 93

Fleischer V, ‘Regulatory Arbitrage’ (2010) 89 Tex L Rev 227

Fleming J Jr, ‘Optimal Deterrence and Accidents’ (1975) 84(4) The Yale Law Journal 656

Haddock D and Macey J, ‘Regulation on Demand: A Private Interest Model, with an Application to Insider Trading Regulation.’ (1987) 30 Journal of Law and Economics 311

Hantke-Domas M, ‘The Public Interest Theory of Regulation: Non-Existence or Misinterpretation?’ (2003) 15 European Journal of Law and Economics 165

Hardin G, ‘The Tragedy of the Commons’ (1968) 162(3859) Science 1243

Hari O and Pasquier U, ‘Blockchain and distributed ledger technology (DLT): academic overview of the technical and legal framework and challenges for lawyers’ (2018) 5 International Business Law Journal 423

Houben Dr R, ‘Cryptocurrencies from a money laundering and tax evasion perspective’ (2019) 30(5) International Company and Commercial Law Review 261

Hughes A and others, ‘Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms’ (2018) Business Horizons 1551 1

Hwaidi Dr M and Ferris G, ‘Switching from Paper to Electronic Bills of Lading: Fundamental Sociological Structure, Distributed Ledger Technology and Legal Difficulties (2019) 24(4) Journal of International Maritime Law 297

Hwaidi M and Ferris G, ‘Switching from paper to electronic bills of lading: Part 2. Fundamental Sociological Structure, Distributed Ledger Technology and Legal Difficulties’ (2020) 25(4) Journal of International Maritime Law 297

Hwaidi M, ‘Letters of credit: model for the illegality exception and for the UCP to address exceptions to the principle of autonomy’ (2021) 32(1) Journal of Banking and Finance Law and Practice 26

Jain G and others, ‘Blockchain for SME Clusters: An Ideation using the Framework of Ostrom Commons Governance’ (2022) 24 Information Systems Frontiers 1125

James O, ‘Regulation Inside Government: Public Interest Justifications and Regulatory Failures’ (2002) 78(2) Public Administration 327

Johnson W, ‘Flexible regulation for dynamic products? The case of applying principles-based regulation to medical products using artificial intelligence’ (2022) 14(2) Law Innovation and Technology 205

Kingsford Smith D, ‘What is Regulation – A Reply to Julia Black’ (2002) 27 Australian Journal of Legal Philosophy 37

Klass G, ‘Intent to Contract’ (2009) 95 Va L Rev 1437

Koo J D, Seong-Hoon Oh and Dong-Chun Lee, ‘Authenticated route optimization scheme for network mobility (NEMO) support in heterogeneous networks’ (2010) 23 International Journal of Communication Systems 1252

Kshetri N, ‘Blockchain’s roles in strengthening cybersecurity and protecting privacy’ (2017) 41 Telecommunications Policy 1027

Kulms R, ‘Blockchains: Private Law Matters’ (2020) Sing JLS 63

Langbroek P and others, ‘Methodology of Legal Research: Challenges and Opportunities’ (2017) 13 (3) Utrecht Law Review

Lasla N and others, ‘Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm’ (2022) 214 Computer Networks, Article 109118

Lee E, ‘Information disclosure and environmental regulation: Green lights and grey areas’ (2010) 4(3) Regulation & Governance Journal 303

Lee R and Ng N, ‘A Tale of Two Common Law Systems: Robinson and Spandeck – Comparing the Test for Duties of Care in Singapore and England (2022) Singapore Comparative Law Review 134

Lee Reed O Jr, 'The Psychological Impact of TV Advertising and the Need for FTC Regulation' (1975) 13 Am Bus LJ 171

Levmore S, ‘Rethinking Ponzi-Scheme Remedies in and out of Bankruptcy’ (2012) 92 BU L Rev 969

Li X and others, ‘A survey on the security of blockchain systems’ (2020) 107 Future Generation Computer Systems 841

Mai F and others, ‘How Does Social Media Impact Bitcoin Value? A Test of the Silent Majority Hypothesis’ (2019) 35(1) Journal of Management Information Systems 19

Masao Y, ‘Virtual currency-regulation and challenges in Japan’ (2017) 32(7) Journal of International Banking Law and Regulation 283

Maxeiner J, ‘When Are Agreements Enforceable? Giving Consideration to Professor Barnett’s Consent Theory of Contract’ (2006) 12 IUS Gentium 92

Mearns E, ‘Vicarious liability for agency contracts’ (1962) 48(1) Virginia Law Review 50

Milunovich G, ‘Assessing the connectedness between Proof of Work and Proof of Stake/Other digital coins’ (2022) 211 Economics Letters, Article 110243

Mohan V, ‘Automated Market Makers and Decentralized Exchanges: A DeFi Primer’ (2022) 8 Financial Innovation, Article 20

Monichino A, ‘Cryptocurrency and interim court relief: Chen v Blockchain Global Ltd, CLM v CLN and Fetch.ai Ltd v Binance’ (2022) 50(3) Australian Business Law Review 205

Morris A, ‘Practical reasoning and contract as promise: Extending contract-based criteria to decide excuse cases’ (1997) 56(1) Cambridge Law Journal 147

Newman H and Wright D, ‘Strict Liability in a Principal-Agent Model’ (1990) 10 International Review of Law and Economics 219

Nicholas B, ‘Force Majeure and Frustration’ (1979) 27 American Journal of Comparative Law 231

Nofer M and others, ‘Blockchain’ (2017) 59(3) Business & Information Systems Engineering 183

Ostrom E, ‘Coping with Tragedies of the Commons’ (1999) 2 Annual Review of Political Science 493

Parry R and Bisson R, ‘Legal approaches to management of the risks of cloud computing insolvencies’ (2020) Journal of Corporate Law Studies 1

Patan R and others, ‘Blockchain Security Using Merkle Hash Zero Correlation Distinguisher for the IoT in Smart Cities’ (2022) 9(19) IEEE Internet of Things Journal 19296

Perry R, ‘The Role of Retributive Justice in the Common Law of Torts: A Descriptive Theory’ (2006) 73 Tennessee Law Review 177

Pia A, ‘Ghosts in the shell: The promises of water users’ associations and the double life of Elinor Ostrom’s design principles in rural China’ (2023) 30(1) Journal of Political Ecology 62

Posch W, ‘Resolving Business Disputes through Litigation or Other Alternatives: The Effects of Jurisdictional Rules and Recognition Practice’ (2004) 26 Houston Journal of International Law 363

Qin R, Yuan Y and Wang F Y, ‘Research on the Selection Strategies of Blockchain Mining Pools’ (2018) 5(3) IEEE Transactions on Computational Social Systems 748

Quang Huynh A N and others, ‘Energy Consumption and Bitcoin Market’ (2022) 29 Asia Pacific Financial Markets 79

Rankin D, Bargum K and Kokko H, ‘The tragedy of the commons in evolutionary biology’ (2007) 22(12) Trends in Ecology and Evolution 643

Reed C, ‘Why Judges Need Jurisprudence in Cyberspace’ (2018) 38 Legal Studies 263

Renn O, ‘Three Decades of Risk Research: Accomplishments and New Challenges’ (1998) 1 Journal of Risk Research 49

Renwick R and Gleasure R, ‘Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems’ (2021) 36(1) Journal of Information Technology 16

Riley J, ‘The Current Status of Cryptocurrency Regulation in China and Its Effect around the World’ (2021) 1 China & WTO Review 135

Sage N, ‘Contractual Liability and the Theory of Contract Law’ (2019) 30(3) King’s Law Journal 459

Salmon J and Myers G, ‘Blockchain and Associated Legal Issues for Emerging Markets’ (Jan 2019) 63 International Finance Corporation 1

Sarkodie S A, Ahmed M Y and Leirvik T, ‘Trade volume affects bitcoin energy consumption and carbon footprint’ (2022) 48 Finance Research Letters, Article 102977

Sarr S, Hayes B and DeCaro D, ‘Applying Ostrom’s Institutional Analysis and Development framework, and design principles for co-production to pollution management in Louisville’s Rebbertown, Kentucky’ (2021) 104 Land Use Policy, Article 105383

Savelyev A, ‘Copyright in the blockchain era: Promises and challenges’ (2018) 34(3) Computer Law and Security Review 550

Schillig M, ‘Lex Cryptographi(c)a, Cloud Crypto Land or What? – Blockchain Technology on the Legal Hype Cycle’ (2023) 86(1) Modern Law Review 31

Schmidt R and Scott C, ‘Regulatory discretion: structuring power in the era of regulatory capitalism’ (2021) 41 Legal Studies 454

Schreuer C, ‘Jurisdiction and Applicable Law in Investment Treaty Arbitration’ (2014) 1 McGill Journal of Dispute Resolution 1

Schwanke A, ‘Bridging the digital gap: How tax fits into cryptocurrencies and blockchain development’ (2017) 28 International Tax Review 20

Scott R, ‘In (Partial) Defense of Strict Liability in Contract’ (2008) 107 Michigan Law Review 1381

Scott T, Ulibarri N and Scott R, ‘Stakeholder involvement in collaborative regulatory processes: Using automated coding to track attendance and actions’ (2020) 14 Regulation and Governance 219

Shackleford S and others, ‘Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices’ (2015) 50(2-3) Texas International Law Journal 305

Sharma P K and Park J H, ‘Blockchain based hybrid network architecture for the smart city’ (2018) 86 Future Generation Computer Systems 650

Shleifer A, ‘Understanding Regulation’ (2005) 11(4) European Financial Management 439

Smith J and Behrman A, ‘The importance of a strong force majeure clause in an unstable geopolitical environment’ (2015) 8(2) Journal of World Energy Law and Business 116

Strauss A, ‘Beyond National Law: The Neglected Role of the International Law of Personal Jurisdiction in Domestic Courts’ (1995) 36 Harvard International Law Journal 373

Strebel E, ‘Caution is key with cryptocurrency’ (2018) Wisconsin Law Journal

Stylianou M, ‘Pure Economic Loss in Negligence: Has England Got It Wrong – Does Australia Have It Right’ (2011) 1 Southampton Student Law Review 20

Tendon S and Ganado M, ‘Legal Personality for Blockchains, DAOs and Smart Contracts’ (2018) 1 Corporate Finance and Capital Markets Law Review 1

Trautman L, ‘Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road and Mt. Gox?’ (2014) 20(4) Richmond Journal of Law and Technology 13

Variale G, ‘Market poll: the best way to regulate’ (2013) Oct International Financial Law Review 1

Wang Y, Zhang M and Kang J, ‘How does context affect self-governance? Examining Ostrom’s design principles in China’ (2019) 13(1) International Journal of the Commons 660

Willoughby T, ‘Domain name disputes: the UDPR 10 years on’ (2009) 4(10) Journal of Intellectual Property Law & Practice 714

Witting C, ‘Duty of Care: An Analytical Approach’ (2005) 25(1) Oxford Journal of Legal Studies 33

Yeoh P, ‘Regulatory issues in blockchain technology’ (2017) 25(2) Journal of Financial Regulation and Compliance 196

Yeung K, ‘Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law’ (2019) 82 (2) The Modern Law Review 207

Zalan T, ‘Born global on blockchain’ (2018) 28(1) Review of International Business and Strategy 19

Zetzsche D, Buckley R and Arner D, ‘The Distributed Liability of Distributed Ledgers: Legal risks of Blockchain’ (2018) University of Illinois Law Review 1361

Zhang J and others, ‘The impact of environmental regulations on urban Green innovation efficiency: The case of Xi’an’ (2020) 57 Sustainable Cities and Society, Article 102123

Zharikov A, ‘Resolving Disputes Without Reference to National Laws: analysis of the nature and practice of Documentary Instruments Dispute Resolution Expertise (DOCDEX)’ (2022) 33(10) International Company and Commercial Law Review 507

Zook M and Blankenship J, ‘New spaces of disruption? The failures of Bitcoin and the rhetorical power of algorithmic governance’ (2018) 96 Geoforum 248

eJournal Articles

Betancourt M, 'Bitcoin (Theory Beyond the Codes)' <https://journals.uvic.ca/index.php/ctheory/article/view/14792/5667> Accessed 1st February 2023

Chalkias K, Chatzigiannis P and Ji Y, 'Broken Proofs of Solvency in Blockchain Custodial Wallets and Exchanges' (2022) Paper 2022/043 Cryptology ePrint Archive <https://eprint.iacr.org/2022/043.pdf> Accessed 1st February 2023

Chapman P and Douglas L, 'The Virtual Currency Regulation Review – Edition 2' (2019) The Law Reviews I <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-2/1197606/united-kingdom> Accessed 1st February 2023

Chatterjee R, 'An Overview of the Emerging Technology: Blockchain' (2017) International Conference on Computational Intelligence and Networks 126 <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8307344> Accessed 1st February 2023

Chohan U, 'Are Stable Coins Stable' (29th March 2020) Notes on the 21st Century (CBRi) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326823> Accessed 1st February 2023

Demertzis M, 'Non-fungible tokens (NFTs): The next chapter in crypto' (January 2022) Bruegel-Blogs <https://go.gale.com/ps/i.do?id=GALE%7CA690531927&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=&p=AONE&sw=w&userGroupName=anon%7Ed2a2fd82> Accessed 1st February 2023

El Menshawy A, 'Mapping Existing Risks and Obstacles to Legal Redress Within Unpermissioned Blockchain Technology' (2022) 10 NIBLeJ 6

Haque R and others, 'Blockchain Development and Fiduciary Duty' (2019) 2 Stanford Journal of Blockchain Law and Policy 139

Parry R, 'Building A Legal Framework to Facilitate The Transformative Potential of Digital Economies' (2022) 10 NIBLeJ 5 <https://www.ntu.ac.uk/__data/assets/pdf_file/0039/1849890/2022-10-NIBLeJ-5.pdf> Accessed 1st February 2023

Shin D, 'Blockchain: The emerging technology of digital trust' (2019) 45 Telematics and Informatics 101278 <https://www.sciencedirect.com/science/article/pii/S0736585319307701> Accessed 1st February 2023

Valeonti F and others, 'Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs)' (2021) 11 Applied Sciences 9931 <https://www.mdpi.com/2076-3417/11/21/9931#cite> Accessed 1st February 2023

Xiong H and others, 'Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms' (2022) 14 Future Internet 47 <http://dx.doi.org/10.3390/fi14020047> Accessed 1st February 2023

Discussion Papers

Alvarez F, Argente D and Van Patten D, 'Are Cryptocurrencies Currencies? Bitcoin as a Legal Tender in El Salvador' (April 2022 – Revised February 2023) working paper 29968 <https://www.nber.org/system/files/working_papers/w29968/w29968.pdf> Accessed 1st February 2023

Ariss P, 'Money for Nothing?' (2017) Credit Management 13 <https://search.proquest.com/docview/1963932998?rfr_id=info%3Axri%2Fsid%3Aprimo&accountid=1469> Accessed 1st February 2023

Black J, 'Constitutionalising Regulatory Governance Systems' (2021) LSE Law, Society and Economy Working Papers 02/2021 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3813812> Accessed 1st February 2023

Bodo B and De Filippi P, 'Trust in Context: The Impact of Regulation on Blockchain and DeFi' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051842> Accessed 1st February 2023

Bordo M and Levin A, 'Central Bank Digital Currency and the Future of Monetary Policy' (August 2017) Working Paper 23711 NBER Working Paper Series <https://www.nber.org/system/files/working_papers/w23711/w23711.pdf> Accessed 1st February 2023

Bullman D, Klemm J and Pinna A, 'In search for stability in crypto-assets: are stablecoins the solution?' (August 2019) No 230 European Central Bank Occasional Paper Series <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3444847> Accessed 1st February 2023

Chohan U W, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1

Gazi S and others, 'Blockchain as Commons: Applying Ostrom's Polycentric Approach to Blockchain Governance' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4250547> Accessed 1st August 2023

Global Legal Research Directorate, 'Regulation of Cryptocurrency Around the World' (2018) The Law Library of Congress, Global Research Centre <https://tile.loc.gov/storage-services/service/ll/llglrd/2018298387/2018298387.pdf > Accessed 1st February 2023

Hays D, 'Blockchain 3.0 The Future of DLT' (2018) June Crypto Research Report, <https://cryptoresearch.report/crypto-research/blockchain-3-0-future-dlt/> Accessed 1st February 2023

Howell B and Potgieter P, 'Regulating Cryptocurrencies: mapping economic objectives and technological feasibilities' (September 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3927658> Accessed 1st February 2023

Jahanshahloo H, Irresberger F and Urquhart A, ‘Bitcoin Under the Microscope’ (November 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4273839> Accessed 1st February 2023

Kapengut E and Mizrach B, ‘An Event Study of the Ethereum Transition to Proof-of-Stake’ (October 2022) <https://arxiv.org/pdf/2210.13655.pdf> Accessed 1st February 2023

Laszka A, Johnson B and Grossklags J, ‘When Bitcoin Mining Pools Run Dry: A Game-Theoretic Analysis of the Long-Term Impact of Attacks Between Mining Pools’ (2015) <http://fc15.ifca.ai/preproceedings/bitcoin/paper_13.pdf> Accessed 1st February 2023

Lourenco A, ‘Autopoietic Social Systems Theory: The Co-evolution of Law and the Economy’ (2010) Working Paper No 409 Centre for Business Research, University of Cambridge <https://www.cbr.cam.ac.uk/fileadmin/user_upload/centre-for-business-research/downloads/working-papers/wp409.pdf> Accessed 1st February 2023

Mamarbachi R, Day M and Favato G, ‘Art as an alternative investment asset’ (2008) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1112630> Accessed 1st February 2023

Moffat N, Srivastava A and Kaplan L, ‘New U.K. Anti-Money Laundering and Counter Terrorist Financing Requirements for Cryptoasset Businesses – Are You Ready?’ (January 2020) <https://www.paulhastings.com/publications-items/details/?id=22d6886e-2334-6428-811c-ff00004cbded> Accessed 1st February 2023

Mondoh B S and others, ‘Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion?’ (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144753> Accessed 1st February 2023

Ostbye P, ‘Exploring DAO Members’ Individual Liability’ (February 2022) Discussion paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4045799> Accessed 1st February 2023

Ostbye P, ‘Exploring The Role of Law in The Governance of Cryptocurrency Systems and Why Limited Liability DAOs might be a Bad Idea’ (January 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007547> Accessed 1st February 2023

Ostbye P, ‘How Are Cryptocurrency Systems Represented and Who is Liable for Misrepresentation?’ (October 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3675083> Accessed 1st February 2023

Ostbye P, ‘Who is Liable for an Attack on Cryptocurrency Consensus?’ (January 2020) <https://kryptografen.com/opinions/who-is-liable-for-an-attack-on-cryptocurrency-consensus/> Accessed 1st February 2023

Ostbye P, ‘Who is Liable if a Cryptocurrency Protocol Fails?’ (September 2019) <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3423681> Accessed 1st February 2023

Porket J L, ‘The Pros and Cons of Government Regulation’ (2003) Institute of Economic Affairs 3rd discussion paper <https://iea.org.uk/wp-content/uploads/2016/07/upldbook341pdf.pdf> Accessed 1st February 2023

Prosser T, ‘Two visions of Regulation: Paper for ‘Regulation in the Age of Crisis’ (2010) <http://regulation.upf.edu/dublin-10-papers/1H1.pdf> Accessed 1st February 2023

Reed QC R (Wilberforce Chambers), ‘Implied contract: a convenient fiction in claiming damages’ (2017) <https://www.wilberforce.co.uk/wp-content/uploads/2017/01/RR-Implied-contract.docx.pdf > Accessed 1st February 2023

Schwinger R, ‘Blockchain Law: When plaintiffs raise claims of platforms behaving badly’ (July 2021) New York Law Journal <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/blockchain-law---when-plaintiffs-raise-claims-of-platforms-behaving-badly.pdf?revision=3fe041d8-c2d6-42f9-913b-0b21c7f53b17&revision=3fe041d8-c2d6-42f9-913b-0b21c7f53b17> Accessed 1st February 2023

Sharma T K, ‘How is blockchain verifiable by public and yet anonymous?’ 10th July 2018 <https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/> Accessed 1st February 2023

Shrestha A K, Vassileva J and Deters R, ‘A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives’ (2020) Frontiers in Blockchain <https://www.frontiersin.org/articles/10.3389/fbloc.2020.497985/full> Accessed 1st February 2023

Wilson S and Chou D, ‘How Healthy is Blockchain Technology’ (2017) Proc HIMSS AsiaPac17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3668102> Accessed 1st February 2023

Wright A and De Filippi P, ‘Decentralized Blockchain Technology and the Rise of Lex Cryptographia’ (2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> Accessed 1st February 2023

Conference Papers

Alsunaidi S and Alhaidair F, ‘A Survey of Consensus Algorithms for Blockchain Technology’ (2019) International Conference on Computer and Information Sciences (ICCIS) <https://ieeexplore.ieee.org/abstract/document/8716424> Accessed 1st February 2023

Bogner A, Chanson M and Meeuw A, ‘A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain’ IoT’16: Proceedings of the 6th International Conference on the Internet of Things (November 2016) 177 <https://doi.org/10.1145/2991561.2998465> Accessed 1st February 2023

Caliskan-Islam A and others, ‘De-anonymizing Programmers via Code Stylometry’ (2015) Proceedings of the 24th Security Symposium <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-caliskan-islam.pdf> Accessed 1st February 2023

Conoscenti M, Vetro A and De Martin J C, ‘Blockchain for the Internet of Things: A systematic literature review’ (2016) IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7945805> Accessed 1st February 2023

Divya K and Usha K, ‘Blockvoting: An Online Voting System Using Block Chain’ (2022) International Conference on Innovative Trends in Information Technology (ICITIIT) (February 2022) <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9744132> Accessed 1st February 2023

Islam M R and others, ‘A Review on Blockchain Security Issues and Challenges’ (2021) IEEE 12th Control and System Graduate Research Colloquium (ICSGRC) 227 <https://ieeexplore.ieee.org/abstract/document/9515276> Accessed 1st February 2023

Kahn A, ‘The Economics of Regulation: Principles and Institutions’ (2012) <https://www.bcuc.com/Documents/Proceedings/2012/DOC_29762_A2-28_Submission.pdf> Accessed 1st February 2023

Reed C, Kennedy E and Nogueira Silva S, ‘Responsibility, Autonomy and Accountability: legal liability for machine learning’ (2016) Microsoft Cloud Computing Research Centre Paper presented at the 3rd Annual Symposium <https://cebcla.smu.edu.sg/sites/cebcla.smu.edu.sg/files/Reed%20Machine%20learning%20liability%20SSRN-id2853462.pdf> Accessed 1st February 2023

Yavuz E and others, ‘Towards secure e-voting using ethereum blockchain’ (2018) 6th International Symposium on Digital Forensic and Security (ISDFS) <https://ieeexplore.ieee.org/abstract/document/8355340> Accessed 1st February 2023

Zhao H (ITU Secretary-General), ‘Collaborative regulation: Special edition, Global Symposium for Regulators (2016) 3 ITU News <https://www.itu.int/en/itunews/Documents/2016-03/2016_ITUNews03-en.pdf> Accessed 1st February 2023

Whitepapers

BitFury Group, ‘Proof of Stake versus Proof of Work White Paper 1.0’ (2015) <https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf> Accessed 1st February 2023

Nakamoto S, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ (bitcoin.org) <https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf> Accessed 1st February 2023

Websites

(bbc.co.uk), ‘Squid Game crypto token collapses in apparent scam’ (November 2021) <https://www.bbc.co.uk/news/business-59129466> Accessed 1st February 2023

(bbc.co.uk), ‘Why the Central African Republic adopted Bitcoin’ (June 2022) <https://www.bbc.co.uk/news/world-africa-61565485> Accessed 1st February 2023

(coinbase.com), ‘What is a stablecoin?’ (2022) <https://www.coinbase.com/learn/crypto-basics/what-is-a-stablecoin> Accessed 1st February 2023

(coinmarketcap.com), ‘Top Cryptocurrency Decentralized Exchanges’ (February 2023) <https://coinmarketcap.com/rankings/exchanges/dex/> Accessed 1st February 2023

(defillama.com), ‘Hacks’ (January 2023) <https://defillama.com/hacks> Accessed 1st February 2023

(docs.kine.im), ‘Terms of Use’ (February 2021) <https://docs.kine.im/library/terms-of-use> Accessed 1st February 2023

(dydx.com), ‘Terms of Use’ (February 2023) <https://dydx.exchange/terms?> Accessed 1st February 2023

(gemini.com), ‘How a Block in the Bitcoin Blockchain Works’ (March 2022) <https://www.gemini.com/cryptopedia/what-is-block-in-blockchain-bitcoin-block-size> Accessed 1st February 2023

(MacroMicro), ‘Bitcoin average Mining costs’ (January 2023) <https://en.macromicro.me/charts/29435/bitcoin-production-total-cost> Accessed 1st February 2023

(Protos.com), ‘Top DeFi hacks and exploits of 2022’ (December 2022) <https://protos.com/top-defi-hacks-and-exploits-of-2022/> Accessed 1st February 2023

(ripple.com), ‘home’ <https://ripple.com/> Accessed 1st February 2023

(sygna.io), ‘Why Regulations Will Benefit the Crypto Industry in the Long Run’ (2020) <https://www.sygna.io/blog/why-regulations-will-benefit-the-crypto-industry-in-the-long-run/> Accessed 1st February 2023

(uniswap.org), ‘Uniswap Labs Terms of Service’ (November 2022) <https://uniswap.org/terms-of-service> Accessed 1st February 2023

Anca F (coindoo.com), ‘The Biggest Crypto Programming Errors in History’ (2019) <https://coindoo.com/the-biggest-crypto-programming-errors-in-history/> Accessed 1st February 2023

Ash T (Addleshaw Goddard), ‘Fetch – The search for information by victims of cryptocurrency fraud’ (Nov 2021) <https://www.addleshawgoddard.com/en/insights/insights-briefings/2021/litigation/the-brief-case-autumn-2021/fetch-the-search-for-information-by-victims-of-cryptocurrency-fraud/#:~:text=In%20Fetch%2C%20the%20Court%20granted,the%20recipients%2C%20innocent%20or%20otherwise%2C> Accessed 1st February 2023

Azati.ai, ‘How Much Does It Cost To Build A Blockchain in 2022’ (January 2023) <https://azati.ai/how-much-does-it-cost-to-blockchain/> Accessed 1st February 2023

Baraniuk C (bbc.co.uk), 'Bitcoin's energy consumption equals that of Switzerland' (3rd July 2019) <https://www.bbc.co.uk/news/technology-48853230> Accessed 1st February 2023

Baraniuk C (BBC), 'Blockchain: The revolution that hasn't quite happened' (2020) <https://www.bbc.co.uk/news/business-51281233> Accessed 1st February 2023

Bartlett J (bbc.co.uk), 'Missing Cryptoqueen: Why did the FCA drop its warning about the OneCoin scam?' (August 2020) <https://www.bbc.co.uk/news/technology-53721017> Accessed 1st February 2023

BBC, 'Bitcoin becomes official currency in Central African Republic' (27th April 2022) <https://www.bbc.co.uk/news/world-africa-61248809> Accessed 1st February 2023

Bbc.co.uk (magazine), 'Who, What, Why: How do you spot a stolen diamond?' (February 2013) <https://www.bbc.co.uk/news/magazine-21525403> Accessed 1st February 2023

binance.com, 'Terms and conditions' <https://www.binance.com/en/terms> Accessed 1st February 2023

bitcoin.com (Avi), 'Who is Satoshi Nakamoto? An Introduction to Bitcoin's Mysterious Founder' (March 2020) <https://news.bitcoin.com/satoshi-nakamoto-founder-of-bitcoin/> Accessed 1st February 2023

bitcoin.org, 'Code Review' <https://bitcoin.org/en/development> Accessed 1st February 2023

bitcoin.org, 'Fixing Existing Issues' <https://github.com/bitcoin/bitcoin/issues> Accessed 1st February 2023

bitcoin.org, 'how to buy bitcoin' <https://bitcoin.org/en/buy> Accessed 1st February 2023

bitcoin.org, 'Minimum Requirements' <https://bitcoin.org/en/full-node#minimum-requirements> Accessed 1st February 2023

bitcoin.org, 'Possible Problems' <https://bitcoin.org/en/full-node#minimum-requirements> Accessed 1st February 2023

bitcoin.org, 'What are the advantages of Bitcoin?' <https://bitcoin.org/en/faq#what-are-the-advantages-of-bitcoin> Accessed 1st February 2023

bitcoin.org, 'Who controls the Bitcoin network?' <https://bitcoin.org/en/faq#who-created-bitcoin> Accessed 1st February 2023

BitGem, 'terms and conditions' <https://www.thediamondloupe.com/sites/awdcnewswall/files/attachments/pinkcoin-sales-terms_0.pdf> Accessed 1st February 2023

Blockchain Council, 'Permissioned and Permissionless Blockchains: A Comprehensive Guide' <https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/> Accessed 1st February 2023

Browne R (cnbc.com), ‘A total disaster: Crypto firms face being booted from the UK as a key deadline approaches’ (March 2022) <https://www.cnbc.com/2022/03/24/crypto-firms-face-being-booted-from-uk-as-fca-register-deadline-nears.html> Accessed 1st February 2023

BTC.com, ‘Pool Distribution’ (January 2023) <https://btc.com/stats/pool?pool_mode=all> Accessed 1st February 2023

Calhoun G (forbes.com), ‘FTX and ESG: A Panorama of Failed Governance (Pt 1 – The Internal Failures)’ (November 2022) <https://www.forbes.com/sites/georgecalhoun/2022/11/21/ftx-and-esg-a-panorama-of-failed-governance-pt-1--the-internal-failures/> Accessed 1st February 2023

Cameron A and Trinh K (theconversation.com), ‘Four factors driving the price of Bitcoin’ (November 2017) <https://theconversation.com/four-factors-driving-the-price-of-bitcoin-87244> Accessed 1st February 2023

Capps D and Collingham F, ‘High Court decided on first English law case on crypto software duties’ (April 2022) <https://www.lexology.com/library/detail.aspx?g=a6a60e6f-d365-45d3-bb99-3bdf505883ce> Accessed 1st February 2023

Castor A and Phillips D (decrypt.co), ‘Curve founder seizes 71% of Curve DAO voting power’ (August 2020) <https://decrypt.co/39599/curve-founder-seizes-71-of-curve-dao-voting-power> Accessed 1st February 2023

cbinsights.com, ‘Banking is only the beginning: 58 big industries Blockchain could transform’ (March 2021) <https://www.cbinsights.com/research/industries-disrupted-blockchain/> Accessed 1st February 2023

cbinsights.com, ‘Banking is only the beginning: 65 big industries blockchain could transform’ (9th March 2022) <https://www.cbinsights.com/research/industries-disrupted-blockchain/> Accessed 1st February 2023

Celsius, ‘Customer Care’ <https://celsius.network/customer-care> Accessed 1st February 2023

Celsius, ‘Why trust Celsius’ <https://celsius.network/why-trust-celsius> Accessed 1st February 2023

citizensadvice.org, ‘Using Alternative Dispute Resolution to solve your consumer problem’ <https://www.citizensadvice.org.uk/scotland/law-and-courts/legal-systems/settling-out-of-court/using-alternative-dispute-resolution-to-solve-your-consumer-problem-s/> Accessed 1st February 2023

coinatmradar.com, ‘Bitcoin ATM Near Me Search’ <https://coinatmradar.com/bitcoin-atm-near-me/> Accessed 1st February 2023

coinbase.com, ‘coinbase user agreement’ <https://www.okex.com/support/hc/en-us/articles/360021813691-Terms-of-Service> Accessed 1st February 2023

Coinfalcon.com, ‘Terms’ <https://coinfalcon.com/en/terms> Accessed 1st February 2023

coingecko.com, ‘Top Cryptocurrency Exchanges Ranking by Trust Score – Spot’ <https://www.coingecko.com/en/exchanges> Accessed 1st February 2023

CoinMarketCap, ‘Top Cryptocurrency Exchanges by Trade Volume (Page 4)’ <https://coinmarketcap.com/rankings/exchanges/4/> Accessed 1st February 2023

Copeland T (decrypt.co), ‘The complete story of the QuadrigaCX $190 million scandal’ (March 2019) <https://decrypt.co/5853/complete-story-quadrigacx-190-million> Accessed 1st February 2023

Coveney D (Interconnectit), ‘How much does code cost?’ (2008) Business <https://interconnectit.com/news/2008/06/01/how-much-does-code-cost/> Accessed 1st February 2023

Cryptimi, ‘How many Cryptocurrency Exchanges are there?’ <https://www.cryptimi.com/guides/how-many-cryptocurrency-exchanges-are-there> Accessed 1st February 2023

cryptonews.com, ‘bitcoin guide’ <https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm> Accessed 1st February 2023

Decrypt.com, ‘The Problem with Decentralized Exchanges – and How to solve it’ (November 2021) <https://decrypt.co/84575/the-problem-with-decentralized-exchanges-and-how-to-solve-it> Accessed 1st February 2023

Dorfman J (Forbes.com), ‘Bitcoin is an Asset, not a Currency’ (2017) <https://www.forbes.com/sites/jeffreydorfman/2017/05/17/bitcoin-is-an-asset-not-a-currency/#6f4277d62e5b> Accessed 1st February 2023

Elderfield M, ‘How to supervise a crypto exchange’ (December 2022) <https://www.ft.com/content/6e2bd1b3-aa4a-40a2-9788-05ced5c1e0fc> Accessed 1st February 2023

Falkon S, ‘The Story of the DAO – Its History and Consequences’ (December 2017) <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee> Accessed 1st February 2023

Fletcher E (ftc.gov), ‘Cryptocurrency buzz drives record investment scam losses’ (May 2021) <https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses> Accessed 1st February 2023

Genc E and Graves S, ’13 Biggest DeFi Hacks and Heists’ (April 2022) <https://decrypt.co/93874/biggest-defi-hacks-heists> Accessed 1st February 2023

Gogo J (beincrypto.com), ‘Top Ten DeFi Hacks of 2022: Hackers Get More Daring’ (September 2022) <https://beincrypto.com/top-ten-defi-hacks-2022-hackers-daring/> Accessed 1st February 2023

Hamilton D (coincentral.com), ‘The Biggest Crypto Programming Errors of All Time’ (2018) <https://coincentral.com/biggest-crypto-programming-errors/> Accessed 1st February 2023

ICANN.org, ‘Uniform Domain-Name Dispute-Resolution’ <https://www.icann.org/resources/pages/help/dndr/udrp-en> Accessed 1st February 2023

iccwbo.org, ‘DOCDEX’ <https://iccwbo.org/dispute-resolution-services/docdex/> Accessed 1st February 2023

ID-3, ‘Cryptographic Key Management – the Risks and Mitigation’ 29th April 2019 <https://id-3.co.uk/cryptographic-key-management-the-risks-and-mitigation/>Accessed 1st February 2023

Kruppa M, ‘DeFi projects rife with hidden risks, global regulatory body warns’ (March 2022) <https://www.ft.com/content/b0c581c8-96b2-4c34-abcc-5189d7283891> Accessed 1st February 2023

Lampert M (Glocalities.com), ‘Global Rise in Environmental Concern’ (2020) <https://glocalities.com/latest/reports/environmental-concern> Accessed 1st February 2023

Libra.org, ‘The Libra Blockchain’ <https://developers.libra.org/docs/the-libra-blockchain-paper> Accessed 1st February 2023

Lindahl B (NordForsk Magazine), ‘Delicate balance between anonymity and law enforcement’ (February 2018) <https://www.nordforsk.org/en/news/delicate-balance-between-anonymity-and-law-enforcement> Accessed 1st February 2023

Lindrea B, ‘Vitalik reveals a new phase in the Ethereum roadmap: The Scourge’ (2022) <https://cointelegraph.com/news/vitalik-reveals-a-new-phase-in-the-ethereum-roadmap-the-scourge> Accessed 1st February 2023

Lugano F, ‘Famous programming errors in the crypto world’ (December 2018) <https://en.cryptonomist.ch/2018/12/08/programming-errors-crypto-world/> Accessed 1st February 2023

Madathil S and Kanduri S, ‘Learn best practices for debugging and error handling in an enterprise-grade blockchain application’ (2022) <https://developer.ibm.com/blogs/debugging-and-error-handling-best-practices-in-a-blockchain-application/> Accessed 1st February 2023

Majaski C (Investopedia), ‘Distributed Ledgers’ (2019) <https://www.investopedia.com/terms/d/distributed-ledgers.asp> Accessed 1st February 2023

McMillan R (Wired.com), ‘The Inside Story of Mt. Gox, Bitcoin’s $460 Million Disaster’ (2014) <https://www.wired.com/2014/03/bitcoin-exchange/> Accessed 1st February 2023

Mellor S, ‘Reflecting crypto craze, crypto-related scams spiral higher in the UK’ (April 2021) <https://fortune.com/2021/04/06/crypto-scams-uk-cryptocurrency/> Accessed 1st February 2023

Mulcahy H, ‘Order, order: Fetch.AI case enhances English Courts’ approach to crypto fraud’ (August 2021) <https://www.fieldfisher.com/en/insights/order-order-binance-case-enhances-english-courts> Accessed 1st February 2023

Nansen.ai, ‘DeFi Statistics [updated in 2023]’ (December 2022) <https://www.nansen.ai/guides/defi-statistics-in-2022> Accessed 1st February 2023

nordvpn.com, <https://nordvpn.com/country/britain/?gclid=Cj0KCQjwm9D0BRCMARIsAIfvfIaIC8STkwpVM1HjnQsp9a0Z_QL2rOkJNlqfMsvTbPvyyAQFGiURroQaAkg7EALw_wcB> Accessed 1st February 2023

okex.com, ‘Terms of service’ <https://www.okex.com/support/hc/en-us/articles/360021813691-Terms-of-Service> Accessed 1st February 2023

Q.ai (forbes.com), ‘What Really Happened To LUNA Crypto’ (September 2022) <https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=68ff269a4ff1> Accessed 1st February 2023

Q.ai (forbes.com), ‘What Really Happened To LUNA Crypto’ (September 2022) <https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=68ff269a4ff1> Accessed 1st February 2023

Roberts D (fortune.com), ‘Behind the “exodus” of bitcoin startups from New York’ (August 2015) <https://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/> Accessed 1st February 2023

Rosic A (blockgeeks.com), ‘17 Blockchain Applications That Are Transforming Society’ (2017) <https://blockgeeks.com/guides/blockchain-applications/> Accessed 1st February 2023

Sanitt A (Norton Rose Full Bright), ‘Smart Contracts’ (November 2019) <https://www.nortonrosefulbright.com/en/knowledge/publications/1bcdc200/smart-contracts> Accessed 1st February 2023

Shaheen H (cryptopolitan.com), ‘OptiFi: Solana-based DEX loses $661,000 due to programming error’ (September 2022) <https://www.cryptopolitan.com/optifi-loses-66100-due-to-coding-error/> Accessed 1st February 2023

Shattered.io <https://shattered.io/> Accessed 1st February 2023

Silverman G (ft.com), ‘SEC explores segregating businesses at crypto exchanges’ (April 2022) <https://www.ft.com/content/efb9e8d5-02c1-4727-a46d-5ad5d34fdf28?accessToken=zwAAAX_5QvO9kdPvuejVAsFHJ9OkbVrV00_fKA.MEYCIQDiRlUDzo2mVDseOKit0_QBjSUVvhmsjg78wP87y-YPqQIhAOJZTbUoZizbYBtQOGPTRKmNaAcnu54RpyVPDoLNhQcC&sharetype=gift?token=33cb1b11-1cd3-4ad9-8bcf-6b1aa24e9bad#comments-anchor> Accessed 1st February 2023

Stevens R (decrpt.co), ‘DeFi: The Ultimate Beginner’s Guide to Decentralized Finance’ (January 2021) <https://decrypt.co/resources/defi-ultimate-beginners-guide-decentralized-finance> Accessed 1st February 2023

Stokes S (Blake Morgan LLP), ‘Digital copyright: AI and Blockchain’ (2019) <https://www.lexology.com/library/detail.aspx?g=f470dbbf-eb8e-44e5-9d45-1f55bfc25e2a> Accessed 1st February 2023

Takemoto Y and Knight S (Retuers.com) <https://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228> Accessed 1st February 2023

Tap.global, 'Terms and conditions' <https://www.tap.global/cryptocurrency-terms-and-conditions> Accessed 1st February 2023

Thake M, 'What's the difference between blockchain and DLT?' (medium.com) <https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd> Accessed 1st February 2023

Tidy J (bbc.co.uk), 'The real victims of mass crypto-hacks that keep happening' (August 2021) <https://www.bbc.co.uk/news/technology-58331959> Accessed 1st February 2023

Tidy J (BBC), 'How a ransomware attack cost one firm £45m' (June 2019) <https://www.bbc.co.uk/news/business-48661152> Accessed 1st February 2023

Toft Madsen J - maersk.com, 'A game changer for Global trade' Sept 2019 <https://www.maersk.com/news/articles/2019/09/20/a-game-changer-for-global-trade> Accessed 1st February 2023

Ward M (BBC), 'Alarming rise is ransomware tracked' (June 2016) <https://www.bbc.co.uk/news/technology-36459022> Accessed 1st February 2023

White G (BBC), 'UK company linked to laundered Bitcoin billions' (March 2018) <https://www.bbc.co.uk/news/technology-43291026> Accessed 1st February 2023

Williams S (Fool.com), '20 Real-World Uses for Blockchain Technology' (2018) <https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx> Accessed 1st February 2023

Wilson T (reuters.com), 'Crime at crypto *DeFi* sites hits $10.5bln in 2021, research shows' (November 2021) <https://www.reuters.com/technology/crime-crypto-defi-sites-hits-105-bln-2021-research-shows-2021-11-18/> Accessed 1st February 2023

Wilson T and Westbrook T (reuters.com), 'Hackers return $260 million to cryptocurrency platform after massive theft' (August 2021) <https://www.reuters.com/technology/defi-platform-poly-network-reports-hacking-loses-estimated-600-million-2021-08-11/> Accessed 1st February 2023

Yaffe-Ballany D (nytimes.com), 'How Sam Bankman-Fried's Crypto Empire Collapsed' (November 2022) <https://www.nytimes.com/2022/11/14/technology/ftx-sam-bankman-fried-crypto-bankruptcy.html> Accessed 1st February 2023

Yang Y (Bloomberg.com), 'Crypto Exchange BitMart Vows Compensation for $150 Million Hack' (December 2021) <https://www.bloomberg.com/news/articles/2021-12-06/crypto-exchange-bitmart-to-compensate-hacked-users-ceo-tweets> Accessed 1st February 2023

Documentaries

Banking on Bitcoin (2016) [documentary] Directed by C. Cannucciari. Netflix

Videos

Collyer Bristow, ‘Financial Services Winter update 2021’ (2nd December 2021) <https://collyerbristow.com/videos/financial-services-winter-update-2021/> Accessed 1st February 2023

Crypto Renegade, ‘Decentralized Exchanges Explained’ (2021) <https://www.youtube.com/watch?v=dgr3yAr2nCE> Accessed 1st February 2023

Simply Explained – Savjee, ‘How does a blockchain work – Simply Explained’ (2017) <https://www.youtube.com/watch?v=SSo_EIwHSd4> Accessed 1st February 2023

TheTruthDrops, ‘World Government Summit 2022: Dr Pippa Malmgren Talks About Blockchain & Digital Currencies’ (2nd April 2022) <https://www.youtube.com/watch?v=cvXdSvja-aI> Accessed 1st February 2023