Mapping Existing Risks and Obstacles to Legal Redress Within Unpermissioned Blockchain Technology

Akrum El MENSHAWY

Introduction:

Unpermissioned blockchain technology, having evolved in an anti-establishment manner,[1] raises the question of whether it can ever be reconciled with existing law. This paper will highlight the existing risks and obstacles that could prevent compatibility with current legal frameworks. Blockchain technology is an emerging technology and topic for academic debate.[2] It has been recognised as having the potential to revolutionise many industries,[3] particularly the financial sector.[4] For those in the computer science industry, blockchain could be viewed as the long-awaited breakthrough for the technological world.[5] Accordingly, it may be said to have developed an aura of perfection amongst users, often referenced as the 'immutability of blockchain'.[6] This concept of immutability refers to the permanence of the ledger and the fact it cannot be altered.[7] 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.[8]

---

[1] 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 15th June 2020, Page 14

[2] Don Shin, 'Blockchain: The emerging technology of digital trust' (2019) 45 Telematics and Informatics 101278 <https://www.sciencedirect.com/science/article/pii/S0736585319307701> Accessed 22nd December 2021, 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 22nd December 2021, Page 126

[3] 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 10th September 2021, Page 4

[4] 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 12th December 2018, 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 June 2018, Page 60

[5] 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

[6] 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 "unchanging through time; unalterable; ageless" "something that is immutable will never change or cannot be changed", see Colllins Dictionary (Online), 'Immutable' <https://www.collinsdictionary.com/dictionary/english/immutable> Accessed 14th April 2020

[7] 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, '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 June 2018, Page 16

[8] 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 25th September 2019, Page 12. Hacking is used in a broad manner in this context.

Despite this perception of safety amongst users, regulators warn of the risks associated with cryptocurrencies that use blockchain technology.[9] The Financial Conduct Authority has even stated that users may "overestimate their knowledge of cryptoassets [that use blockchain technology]".[10] 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.

Blockchain technology has wide-ranging potential applicability.[11] Not only has its use increased but the methods of how users interact with the technology continue to develop. This will be covered in more depth in due course. The key aspect to note here is that as the methods of interaction and use increase, 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".[12] 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."[13] This notion of risk is capable of application within the field of technology.[14] In this paper, the 'risk' discussed will be elements that pose a threat to the notion of immutability. By stating the obstacles to legal redress, this paper will highlight barriers to 'legal mitigation' of the consequences of these risks.

This paper will therefore provide an analysis of the threats to the immutability of unpermissioned blockchain technology. Three main risks that threaten this notion will be raised in the form of exchange hacks, cryptographic key theft and dishonest nodes. The paper will also highlight the two main obstacles to legal redress for such risks, which are the degree of anonymity present and the jurisdictional issues that arise. Therefore, this paper seeks to establish that the technology has risks and not just the cryptocurrencies that use blockchain. Furthermore, if regulators wish to intervene, unique approaches may be needed to deal with the different methods of interaction with unpermissioned blockchain technology.

What is unpermissioned blockchain technology?

Before exploring the risks and obstacles to legal redress, there must first be an understanding of the key terminology within this field. Unpermissioned blockchain technology is merely a type of Distributed Ledger Technology (hereby DLT). Within the term DLT there are two concepts, a distributed ledger and the technology element. A distributed ledger can be defined as "an asset database that can be shared across a network of multiple sites, geographies or institutions."[15] DLT 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

[9] Ibid, Page 11
[10] Ibid
[11] 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 22nd December 2021
[12] Ortwin Renn, 'Three Decades of Risk Research: Accomplishments and New Challenges' (1998) 1 Journal of Risk Research 49, Page 51
[13] Ibid
[14] 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
[15] Government Office for Science (2008). *Distributed Ledger Technology: beyond block chain*, Accessed 5th February, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>, Page 5

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."[16]

DLT operates via "networks of databases that allow participants to create, disseminate and store information."[17] DLT's vast potential, and possible threats that it presents, are not in themselves new concepts. DLT has been around for multiple decades.[18] However, due to its limited usage, it remains a rather novel invention.[19] For those in the computer science industry, DLT has been treated as a long-awaited breakthrough for the technological world.[20] DLT has the potential to change many industries by enabling transactions to take place peer-to-peer, securely and without the need for a trusted third party to authenticate the transaction. The broad spectrum of uses of DLT is not the focus of this paper. Similarly to a traditional ledger,[21] a distributed ledger requires updating after each transaction. However, this can only be achieved in DLT through a process known as consensus. 'Consensus' requires the whole network to accept the updated transaction, unlike in a traditional ledger whereby an individual could update the ledger without consensus.[22]

Consensus is heavily reliant on the validation process, which is used to determine the trustworthiness of a transaction (its validity). This includes concepts such as whether the property transferred belongs to the seller and whether the property exists. The vital aspect of the validation process is mining. Mining is the completion of complex cryptographic algorithms for validation in the return of a virtual token. In Bitcoin for example, the reward is Bitcoin.[23] Validation nodes attempt to complete these algorithms to ensure that the transaction is valid with the virtual token as the incentive. This computational process is costly from a monetary and time perspective but is essential. Without it, the validity of transactions would be difficult to determine which prevents consensus from being reached. This issue of consensus is important from an operational aspect for DLT but also highlights how different it is from traditional bi-party ways of contracting. Often bi-party contractual agreements are reliant on a third party. For example, in the sale of land in England, the sale must be registered with the Registry Office.[24]

---

[16] Ibid

[17] 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 June 2018, Page 10

[18] Simply Explained – Savjee, 'How does a blockchain work – Simply Explained' (2017) <https://www.youtube.com/watch?v=SSo_EIwHSd4> Accessed 23rd July 2018, Minute 0:18-0:27

[19] 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

[20] (n5)

[21] According to the Cambridge Dictionary (2020) Accessed 6th February 2020 <https://dictionary.cambridge.org/dictionary/english/ledger> 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.

[22] Christina Majaski (Investopedia), 'Distributed Ledgers' (2019) <https://www.investopedia.com/terms/d/distributed-ledgers.asp> Accessed 20th November 2019

[23] (n3), Page 5

[24] Dent Bostick, 'Land Title Registration: An English Solution to an American Problem' (1987-1988) 63 Indiana Law Journal 55, Pages 90-93

Whilst there are a few variations of DLT,[25] blockchain technology is the most relevant for this paper. There are two main forms of blockchain technology: permissioned blockchain technology and unpermissioned blockchain technology (also referred to as permissionless blockchain technology).[26] Due to the presence of a central party, 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 technology is Maersk.[27] 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." This can also indicate that permissioned blockchain technology is capable of being used in orthodox commercial activities where there is a clear legal framework in the form of contract law. 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. The ability to control private information is important as some information in a commercial setting may be especially sensitive due to contractual agreements for example. This remains an example of usage for permissioned blockchain technology but more exist.[28] In theory, any company wanting a uniform ledger could implement permissioned blockchain technology.[29]

Conversely, in a platform using unpermissioned blockchain technology, consensus is a complex and costly process. Theoretically, any participant with the necessary computational power can act as a validation node for an unpermissioned blockchain. Often this costly task is compensated with virtual tokens in the process of mining. In Bitcoin for example, the miners/validation nodes would receive a specified amount of Bitcoin for the completion process of mining each new block. This paper focuses on unpermissioned blockchain technology as it provides a more unique platform for legal analysis due to the lack of a centralised party.

Unpermissioned blockchain technology is far removed from that of a permissioned blockchain. Unpermissioned blockchain technology is extremely novel and untraditional because it does not require a centralised party. In many circumstances, a centralised party such as a bank is required to authenticate transactions and to update and maintain the system. One example of such a requirement is through the use of documentary credits in international

[25] For a discussion of Directed Acyclic Graphs and hybrid strands of DLT see, Demelza Hays, 'Blockchain 3.0 The Future of DLT' (2018) June Crypto Research Report, Accessed 6th February 2020 <https://cryptoresearch.report/crypto-research/blockchain-3-0-future-dlt/> Section 'The Blockchain Solution That is Not a Blockchain'

[26] (n17), Pages 20-21

[27] 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 21st February 2020) in 2018 that was made possible through the use of Permissioned blockchain technology.

[28] Another example would include Ripple. Ripple contains a cryptocurrency in the form of XRP and also 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 21st February 2020

[29] 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 20th Febraury 2020

trade.[30] The use of an intermediary in international trade is vital to offer "a high level of protection and security to both buyers and sellers… The seller is assured that payment will be made by a party independent of the buyer so long as the terms and conditions of the credit are met. The buyer is assured that payment will be released to the seller only after the bank has received the title documents called for in the credit."[31] Trust is therefore placed in the bank as parties in international trade may not have developed 'trust' in the parties they are dealing with.

This paper therefore focuses solely on unpermissioned blockchain technology in this context as permissioned blockchain technology effectively introduces an intermediary. Unpermissioned blockchain technology removes the need for this centralised party and instead relies upon cryptographic technology to validate the transactions.[32] The maintenance and upkeep of the system are distributed equally between the network's participants with the responsibility theoretically shared. It is clear from the examples given above that permissioned and unpermissioned blockchain technology differ in operation. However, the term blockchain is still commonly misused as an all-encompassing term. Occasionally there is even the incorrect use of the key terms.[33] This may indicate that blockchain technology is highly complex and therefore difficult to understand.[34] Furthermore, there is the notion of uncertainty of how or indeed whether various sectors could embrace such a technology that remains widely unexplored.[35] There is a greater degree of scepticism and uncertainty with unpermissioned blockchain technology rather than permissioned blockchain technology.

Due to the presence of the central party in permissioned blockchain technology, it is likely to conform to legal frameworks more easily. Unpermissioned blockchain technology however raises more legal questions and enhances this legal uncertainty. Currently, cryptocurrencies seem to be the most prominent use of unpermissioned blockchain technology with Bitcoin being the most well-known example here. For example, the prominence of Bitcoin highlights individuals' willingness to engage in a platform using unpermissioned blockchain technology. There is a recognition of the presence of 'risks' and volatility within cryptocurrencies, however, the notion of immutability for the technology remains. This in turn can be a dangerous element for users if the potential of hacking is not seen as a significant threat due to the use of unpermissioned blockchain technology.

How do users interact with unpermissioned blockchain technology?

Further complicating the area of study, unpermissioned blockchain technology has several ways in which individuals can interact with it. For this paper, the focus will be on how

---

[30] "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), Paper 10, Page 50. For further discussion of documentary 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 Journal of Banking and Finance Law and Practice 26

[31] 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), Paper 10, Page 50

[32] (n17), Page 20

[33] 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

[34] Alex Hughes, Andrew Park, Jan Kietzmann and Chris Archer-Brown, 'Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms' (2018) Business Horizons 1551 1, Page 7; (n19), Page 425

[35] Alex Hughes, Andrew Park, Jan Kietzmann and Chris Archer-Brown, 'Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms' (2018) Business Horizons 1551 1, 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 March 2020

individuals have interacted with the cryptocurrencies that utilise the technology. There are three important ways that individuals have accessed cryptocurrencies for this paper: the peer-to-peer method, the exchange and the DeFi Exchange[36] (herby referred to as DEXs).[37] The peer-to-peer method operates directly on the blockchain and therefore does not require a central party.[38] Due in part to the technical nature of the peer-to-peer method, many users have interacted via an exchange. According to CoinMarketCap, there are over four hundred cryptocurrency exchanges, and this figure has risen over recent years.[39] Within the cryptocurrency market, some exchanges themselves have become decentralised and are referred to as DEXs.[40] "A DEX provides agents with the opportunity to exchange one asset for another without a centralised third-party responsible for overseeing trading activity."[41] It has also been referred to as 'atomic swaps' whereby the swap will only happen once both parties have agreed to release their cryptocurrency.[42]

Further exploration of the operation of these three methods is beyond the scope of this paper. The key point to acknowledge here is that users may interact in a variety of ways with unpermissioned blockchain technology. Each method differs from one another significantly and may require different legal approaches. However, this notion of immutability for unpermissioned blockchain technology remains. The next section will explore the three main risks to this notion of immutability that are present within unpermissioned blockchain technology bearing in mind the different methods of interaction.

Risks:

Before understanding the three key risks, we must first recognise the key aspects that create such a notion of safety against hacks. 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 intended party.[43] 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.

---

[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' (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3722714> Accessed 7th December 2021, Page 1

[37] Additional methods of purchasing cryptocurrencies exist, for example Bitcoin ATMs. For further information on this, see bitcoin.org, 'how to buy bitcoin' <https://bitcoin.org/en/buy> Accessed 21st November 2019

[38] (n17), Page 87

[39] (coinmarketcap.com), 'Top Cryptocurrency Spot Exchanges' <https://coinmarketcap.com/rankings/exchanges/> Accessed 27th December 2021. The same site in 2019 stated over three hundred exchanges were being tracked by them, see CoinMarketCap, 'Top Cryptocurrency Exchanges by Trade Volume (Page 4)' <https://coinmarketcap.com/rankings/exchanges/4/> Accessed 5th December 2019

[40] (n36)

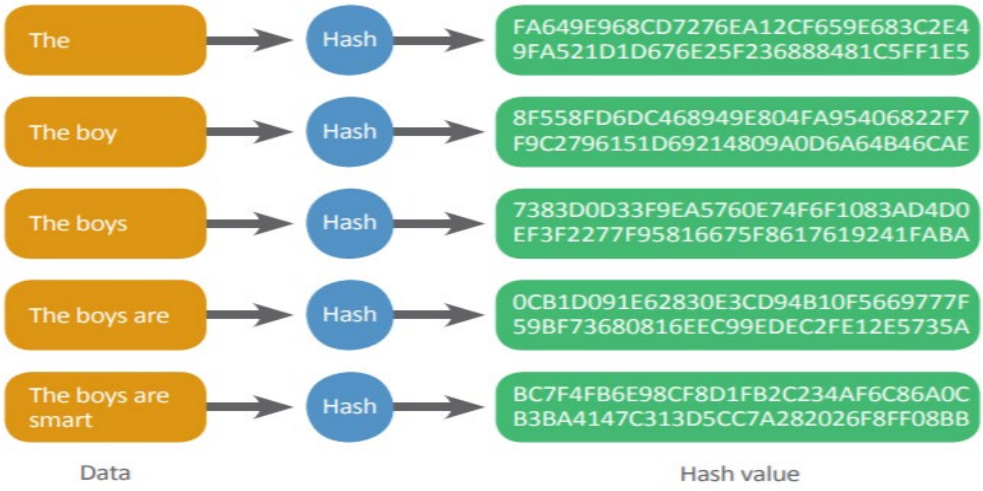
[41] Vijay Mohan, 'Automated Market Makers and Decentralized Exchanges: A DeFI Primer' (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3722714> Accessed 7th December 2021, Page 3

[42] 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 7th December 2021, Page 9

[43] "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 2nd April 2020

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".[44] The threat of this private key being stolen will be discussed later in this paper.

Additionally, the unique hash code created for each addition or alteration to the platform is another aspect of the security of unpermissioned blockchain technology.[45] 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 associated.[46] 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 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 it is not bound to the previous one then it means it is not a valid transaction.[47] As a result, it makes "unauthorised changes… very difficult, if not impossible."[48] For a visual representation of how the hash code can develop please see figure 1 below.



Example of the generation of a SHA256 hash for different character strings

Figure 1: Hash code example (HKMA 2016 Whitepaper on Distributed Ledger Technology 1.0)[49]

Figure 1 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 being able to predict how the hash

[44] Alex Hughes, Andrew Park, Jan Kietzmann and Chris Archer-Brown, 'Beyond Bitcoin: What blockchain and distributed ledger technologies means for firms' (2018) Business Horizons 1551 1, Page 4

[45] It may even be regarded as the most pivotal aspect to the security of any platform using unpermissioned blockchain technology. See (n17), Page 16

[46] Ibid, Page 5

[47] For example someone is attempting to transfer property that either does not exist or does not belong to the one seeking to transfer it. As a result, any attempt to interfere with the information such as maliciously attempting to change the record of ownership, shall render all the previous sets of information invalid, as the hash will alter and no longer bind itself to the previous hashes. For more discussion of this see (n18)

[48] (n17), Page 5

[49] Ibid, Page 23

code would be randomly generated for each new block.[50] It must be noted that there is the possibility that the hash could be broken by brute force, although this is highly difficult.[51]

Another key element to the immutability of unpermissioned blockchain technology is proof-of-work as it is a key component to validation.[52] Proof-of-work seems to be the most used method of validation within unpermissioned blockchain technology.[53] More recently there is the introduction of proof-of-stake as an alternative to proof-of-work.[54] A detailed discussion of these protocols would not benefit this paper.[55] 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 the lack of a centralised party could cause issues for validation. Proof-of-work enables the validity to be secure and legitimate.[56] It includes the complex computerised algorithm that must be run for blocks to be added.[57] This intentionally slows down the validation process.[58] In Bitcoin for example, proof-of-work amounts to roughly ten minutes.[59] Such a delay is regarded as an ideal balance in slowing the process down enough to validate accurately without making it impractical for transactions to take place.[60] Now that some of the key elements to the security of unpermissioned blockchain technology have been discussed, focus can be made on the key threats to immutability.

Hacking:

The main threat to immutability is hacking. Currently, all the reported hacks within the cryptocurrency sector have been hacks of the exchanges or DEXs and not direct hacks of the peer-to-peer method.[61] As a result, it appears that the peer-to-peer method may more enticing from a security perspective. However, as referenced previously the peer-to-peer method is not the only way people interact with unpermissioned blockchain technology. Therefore, to state that unpermissioned blockchain technology is immutable, it must be true of the various methods of interaction. The exchange method and DEXs have been susceptible to hacks and scams and so could provide a significant risk for users and a threat to the notion of immutability.

---

[50] Alexander Savelyev, 'Copyright in the blockchain era: Promises and challenges' (2018) 34(3) Computer Law and Security Review 550, Page 554

[51] Shattered.io <https://shattered.io/> Accessed 4th January 2022

[52] (n50), Page 559

[53] 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 30th December 2021, Pages 5-6

[54] 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.

[55] For more information on proof-of-stake see (n19), Page 427

[56] Michael Nofer, Peter Gomber, Oliver Hinz and Dirk Schiereck, 'Blockchain' (2017) 59(3) Business & Information Systems Engineering 183, Page 184

[57] "*Proof-of-Work* implies that the miner has to resolve extremely complex mathematical problems that are also expensive in terms of energy consumption" see (n19), Page 427

[58] (n18), Minute 3:12-3:17

[59] Ibid, Minute 3:18-3:25

[60] 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

[61] 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; Dirk Zetzsche, Ross Buckley and Douglas Arner, The Distributed Liability of Distributed Ledgers: Legal risks of Blockchain (2018) University of Illinois Law Review 1361, 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 7th December 2021

One of the most prominent examples of a cryptocurrency exchange hack was the hack of Mt. Gox.[62] The mismanagement of the then industry-leading exchange resulted in nearly half a billion dollars worth of Bitcoin (in 2014) being stolen, Federal investigations, and lawsuits galore.[63] In August 2021, a DEX was hacked and over six hundred million dollars worth of cryptocurrency was stolen.[64] Some estimates suggest that such hacks of DEX platforms in 2021 alone have totalled over ten billion dollars.[65] Highlighting every single hack or scam of exchanges and DEXs would provide little benefit for this paper. In highlighting these examples it indicates that the threat of hacking within unpermissioned blockchain technology exists particularly when considering the various methods of interaction.

For customers of the exchange or DEX, there is a possibility that they could pursue the exchange or DEX itself. The presence of the central party (exchange or DEX) increases the ease of legal enforcement.[66] However, liability will likely be restricted significantly in the terms and conditions of those platforms.[67] 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 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.[68] The only signifier of 'ownership' on the peer-to-peer method that an individual would have is their private key. However, once the property was transferred the private key would not be attached to it anymore. This may leave those customers who have suffered losses with limited legal protection. Another potential issue could be raised in this context, which is based on the importance of the use of cryptographic keys and shall be discussed in the following section.

Cryptographic key theft:

One way to attempt to determine property ownership is by cryptography, although this can also cause some issues for immutability.[69] Cryptographic key theft is another layer of security risk that could affect users irrespective of the method of interaction with unpermissioned blockchain technology. The concept of cryptography has been discussed in a previous section and so will just be lightly touched upon here. If individuals forget their private

---

[62] 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 November 2021

[63] Yoshifumi Takemoto and Sophie Knight (Retuers.com) <https://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228> Accessed 1st November 2021; 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 November 2021

[64] 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 7th December 2021

[65] 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 7th December 2021

[66] (n42), Page 17

[67] For an example, see binance.com, 'Terms and conditions' <https://www.binance.com/en/terms> Accessed 14th September 2020, Part IV Sections 2-3

[68] 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 8th January 2022; 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 8th January 2022

[69] 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

key, there is no central system or administrator they can recover it from. Also, how they store the information for the private key must be secure.[70] Hackers could seek to use malware to infiltrate individuals' storage of their private keys.[71] Once accessed, the hackers would be able to use the private key to access the accounts and transfer the property 'legitimately'. The use of the term legitimate here regards the fact that there would be no way for unpermissioned blockchain technology to decipher that it wasn't a legitimate transaction.

There are also potential privacy issues that could arise with cryptography; however, this is beyond the scope of this paper. Hacking of exchanges and theft of the private key are not the only threats to the immutability within unpermissioned blockchain technology. The next section will explore the reliance placed on the trustworthiness and honesty of the validating nodes.

The honesty of the validating nodes:

The final alternative form of 'hacking' is reliant on the validating nodes within a platform using unpermissioned blockchain technology. This references the infamous '51% attack'.[72] Satoshi Nakamoto, a pseudonym of the creator of Bitcoin,[73] highlights that one issue with 'third-party electronic payment systems' is the reliance of trust placed on the intermediaries.[74] Consequently, Satoshi suggests that his centralised system renders the need for those intermediaries to act as mediators and therefore possess the capability to reverse transactions accordingly.[75] In the concept raised by Satoshi, this trust in the intermediary is theoretically replaced with cryptography.[76] However, there is a consequential degree of trust placed on the validating nodes, who although not operating in the mediating role, still have a degree of trust placed upon them. 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."[77]

In any platform that uses unpermissioned blockchain technology the incentive to 'mine' and validate transactions must be sufficient.[78] Often in cryptocurrencies, the coins are the incentive.[79] This is vitally important to encourage a high enough volume of mining, to enable the platform to run quickly.[80] In a platform using unpermissioned blockchain technology, whilst the responsibility theoretically is shared amongst participants, in reality, there is no obligation on any participant to maintain, update and validate for the network.

---

[70] Nikita Storublevtcev, 'Cryptography in Blockchain' in S Misra Et Al (eds) *Computational Science and Its Apllications – ICCSA* (Springer Nature 2019), <https://link.springer.com/paper/10.1007/978-3-030-24296-1_39#citeas> Accessed 28th December 2021, Page 498

[71] Dhavala Lalitha Bhaskari and PSG Aruna Sri, 'A study on blockchain technology' (2018) 7 (2.7) International Journal of Engineering & Technology 418, Page 419

[72] Shikah Alsunaidi and Fahd Alhaidair, 'A Survery of Consensus Algorithms for Blockchain Technology' (2019) International Conference on Computer and Information Sciences (ICCIS) <https://ieeexplore.ieee.org/abstract/document/8716424> Accessed 28th December 2021, Part III

[73] For more information on the theory of who could be Satoshi, see Banking on Bitcoin (2016) [documentary] Directed by C. Cannucciari. Netflix.

[74] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (bitcoin.org) <https://bitcoin.org/bitcoin.pdf> Accessed 12th October 2019, 1.0 Introduction

[75] Ibid

[76] Ibid

[77] Ibid

[78] Michael Betancourt, 'Bitcoin (Theory Beyond the Codes)'<https://journals.uvic.ca/index.php/ctheory/article/view/14792/5667> Accessed 1st January 2019, Page 1 Para 4

[79] Melanie Swan, Blockchain: Blueprint for a New Economy (O'Reilly 2015), Page X

[80] The speed of the system is seen as one of the undeniable advantages of blockchain overall and so ensuring this speed is key in unpermissioned blockchain technology. For further information see (n8), Page 11

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 in normal contractual settings is both the remuneration and the desire to not be sued for falling below the obligations. This contractual arrangement 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.[81] 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 that the threat of this 51% attack has not seemingly materialised in platforms using unpermissioned blockchain technology.[82]

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 a hacking intention. There is the additional element that in Bitcoin for example, there are a few mining pools that have a large degree of 'indirect control' over the validation process of the network and so this could potentially increase the risk of such an attack.[83] Some calculations of blocks mined on the Bitcoin blockchain suggest that almost 70% of the mined blocks have been done by 'mining pools'.[84] Almost half of those have been fulfilled by five mining pools alone.[85] Other suggestions claim that 75% of the network is currently controlled by 'mining pools', most of which are based in China.[86] This could mean that if a 51% attack was sought after, it would not necessarily involve a significant number of individuals 'dishonestly validating', but merely a collection of these mining pools.

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 provide targets for hackers to exploit. However, this is not the only area that unpermissioned blockchain technology may suffer because of. Cryptographic key theft, as discussed above, and the potential for a pool of malicious nodes to overpower the honest nodes remain areas of concern for unpermissioned blockchain technology. These areas may even be the subject of increased academic debate in the future, but further exploration of these possibilities is beyond the scope of this paper.

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 both from a regulatory perspective and for users. Consequently, this paper states that due to the common use of intermediaries in unpermissioned blockchain technology, it cannot be said to guarantee immutability. It is important to note that the exchanges and DEXs may be involved in the cryptocurrency transactions but cannot be blamed for problems of the peer-to-peer method should they arise. Whilst the peer-to-peer method appears secure, due to cryptography and verification safeguards, the way it is commonly used gives rise to vulnerability from hacks and cryptographic key theft for example.

---

[81] (n78), Page 1 Paras 3-5

[82] (n72)

[83] Dirk Zetzsche, Ross Buckley and Douglas Arner, 'The Distributed Liability of Distributed Ledgers: Legal risks of Blockchain' (2018) University of Illinois Law Review 1361, Page 1380

[84] BTC.com, 'Pool Distibution' <https://btc.com/stats/pool?pool_mode=all> Accessed 30th November 2021

[85] F2 Pool – 9.4%, AntPool – 8.4%, BTC.com – 5.2%, SlushPool – 5.0% and BTC Guild – 4.6%, see Ibid

[86] 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

Obstacles to legal redress:

The issue of Anonymity

It is clear from the previous sections that risks of 'hacking' exist due to the various methods of interaction with the technology. 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 can be discussed here. It has been noted that anonymity is a fundamental characteristic of unpermissioned blockchain technology.[87] 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 that is permitted.[88] Pseudonymous is defined as "using a false name".[89] This is in contrast to anonymous whereby no name is given. This therefore can apply to unpermissioned blockchain technology as participants are somewhat identifiable via their IP addresses. However, Virtual Private Network (VPN) can be used to hide or mimic false locations which can render identify effectively anonymous.[90] It does this by technically connecting you to a 'false server' in a different location. This can be used for streaming activity while abroad or finding cheaper tickets for flights. The point in highlighting this is not to suggest that there is an issue with VPN themselves. However, with the limited identification of the real-world identity of the user already prevalent in unpermissioned blockchain technology, true anonymity is certainly possible. As a result, there is a clear possibility of anonymity within unpermissioned blockchain technology and this can be a key obstacle for legal redress.

The key part to understand is the impact that such a possibility of anonymity can have on society. In this paper, 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.[91] To some extent, the regulatory approach is not the major issue. Instead, it is the practicality of such an approach and whether it can overcome the unique characteristics of unpermissioned blockchain technology such as anonymity. This is not only an issue from a regulatory perspective but also from the perspectives of the users. Whilst legal rights could theoretically arise even when the party at fault is unknown, it would be difficult to seek legal

---

[87] 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 7th April 2020; (n5)

[88] Dr Robby Houben, 'Cryptocurrencies from a money laundering and tax evasion perspective' (2019) 30(5) International Company and Commercial Law Review 261, Page 263

[89] Collin dictionary, 'Pseudonymous' (2020) <https://www.collinsdictionary.com/dictionary/english/pseudonymous> Accessed 16th June 2020

[90] For example, a company such as Nord VPN offers the capability to "go truly private" and to "take privacy into your own hands", see nordvpn.com, <https://nordvpn.com/country/britain/?gclid=Cj0KCQjwm9D0BRCMARIsAIfvfIaIC8STkwpVM1HjnQsp9a0Z_QL2rOkJNlqfMsvTbPvyyAQFGiURroQaAkg7EALw_wcB> Accessed 13th April 2020

[91] 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 14th April 2020

redress if parties are anonymous in unpermissioned blockchain technology.[92] Further discussion of the practical issues in pursuing a claim when the parties are unknown is beyond the scope of this paper.[93] The key aspect here is that the anonymity that is possible within unpermissioned blockchain technology provides an additional element of consideration and can provide a significant obstacle for legal redress.

Unpermissioned blockchain technology enables anonymity so it may be problematic for any transfer to take place with the certainty that the receiver 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 party for example a bank at fault even in situations where the bank should have been on inquiry as to the transfers.[94] However, in a platform using unpermissioned blockchain technology not only is there no centralised party 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.

In a platform that uses unpermissioned blockchain technology, the private cryptographic key is vital to ensure that the party receiving the property is the intended party.[95] As stated previously, the use of cryptographic keys is vital to ensure that although anonymity may exist, there remains a degree of security and trust that only the party to whom the property is transferred will be able to access it with their private key. For this paper, the use of cryptography seems to provide sufficient protections concerning this aspect. However, the presence of anonymity remains a key obstacle for legal redress.

It seems relevant at this point to highlight the potential for growing obscurity of the capability for anonymity within unpermissioned blockchain technology. Unpermissioned blockchain technology has evolved and so should not be viewed solely as a disruptive technology'.[96] Unpermissioned blockchain technology and its early uses were designed in an anti-establishment manner.[97] 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 technologies have since evolved from anti-establishment digital currencies operating outside mainstream financial systems to a 'revolutionary' technological blueprint for distributed

---

[92] For example in Hamid v Francis Bradshaw Partnership [2013] EWCA Civ 470, Lord Justice Jackson upholds 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.

[93] For a discussion into the *Fetch.ai* v *Persons Unknown and Others* [2021] EWHC 2254 (Comm), 2021 WL 03605514 case whereby anonymous fraudsters of a cryptocurrency exchange were pursued, see Collyer Bristow, 'Financial Services Winter update 2021' (2nd December 2021) <https://collyerbristow.com/videos/financial-services-winter-update-2021/> Accessed 7th December 2021, Minutes 37-51

[94] 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 upholds 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.

[95] "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 2nd April 2020

[96] (n3), Page 14

[97] (n1)

computing architectures, such as Ethereum."[98] Therefore, as the use of blockchain technology continues to evolve, the obstacle of anonymity in unpermissioned blockchain technology may become less pertinent if more platforms use permissioned blockchain technology as a way to operate within traditional establishments.[99] However, the potential for unpermissioned blockchain technology to be used and the potential for anonymity within these decentralised blockchains remain. Consequently, the potential of anonymity within unpermissioned blockchain technology provides an obstacle for legal redress and must be considered in future regulatory debates.

Jurisdictional complications:

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.[100] This can be regarded as a strength of the technology as it responds to the globality of business and can reduce costs and increase efficiency.[101] However, it can also amount to an obstacle for legal redress as it can create a degree of legal uncertainty. Similarly to the issue of anonymity, this will be a key problem that regulators must seek to clarify if legal clarity can prevail.[102]

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.[103] However, a global convention is not always practicably viable.[104] Due potentially to factors such as religion, culture, and politics there are wide-ranging approaches[105] and opinions on the legal approach that should be taken with cryptocurrencies, blockchain or more specifically unpermissioned blockchain technology.[106]

The difficulty of achieving consensus in regulation 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.[107] In the absence of a convention, uncertainty of 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 paper. As a result, this section will provide a hypothetical situation, to highlight key

---

[98] 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

[99] 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 15th June 2020

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

[101] Ibid

[102] (n19), Page 444 "When the anonymity of participants is concerned, complex questions arise in relation to applicable laws and competent jurisdictions."

[103] Tonya Evans, 'Role of International Rules in Blockchain-Based Cross-Border Commercial Disputes' (2019) 65 Wayne Law Review 1, Pages 7-8

[104] 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

[105] 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 28th January 2021. '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.

[106] (n50), Page 559

[107] For a discussion of how an international treaty can impact the application of applicable and jurisdicitional law see, Christoph Schreuer, 'Jurisdicition and Applicable Law in Investment Treaty Arbitration' (2014) 1 McGill Journal of Dispute Resolution 1

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.

Applicable law

In a traditional setting, two layers of law would need to be determined before legal redress can be granted.[108] These two layers are applicable law and jurisdictional law. The relationship between them is often important in seeking legal redress.[109] This is both from the regulatory perspective and the perspective of the individual seeking legal redress. The first one mentioned is the applicable law. This means the terms that govern the conduct.[110] 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.[111] 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 was raised in England, the courts would interpret the contract in line with English law unless a different Country's law was agreed by the parties.[112] 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.

In the peer-to-peer method of interaction, there exists 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'.[113] 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."[114] The internal rules are unlikely to contain the intention to be legally bound and so the applicability of contract law is limited.[115] Courts have long recognised that words and actions of the party will be used to determine their contractual intent through an objective standard.[116] 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

---

[108] Ibid, Page 2

[109] 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

[110] (n107), Page 2; Ibid, Page 376

[111] *Modahl* v *BAF* [1992] 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 8th January 2022

[112] *Beximco Pharmaceutical Ltd* v *Shamil Bank of Bahrain EC* [2004] EWCA Civ 19; *Halpern* v *Halpern* [2007] EWCA Civ 291

[113] 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

[114] John Salmon and Gordon Myers, 'Blockchain and Associated Legal Issues for Emerging Markets' (Jan 2019) 63 International Finance Corporation 1, Page 4

[115] 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), Paper 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

[116] *Storer* v *Manchester City Council* [1974] 1 WLR 1403, Para 1408

against involving the law.[117] As the responsibility for maintenance and upkeep in unpermissioned blockchain technology is distributed equally amongst its participants, in theory no participant is more at fault than another.[118] From a practical perspective, it would be very difficult also to pursue the whole network. 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 or factors such as foreseeability, proximity and reasonableness which can be considered to determine if a duty should exist.[119] The traditional *Caparo* test has been overturned in *Robinson* (2018)[120] 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."[121] Some pre-established relationships can include "motorists to other road users…manufacturers to consumers…employers to their employees, and…doctors to their patients"[122] to name a few. If cases are brought in tort in the context of unpermissioned blockchain technology, it is likely that this approach of incremental development will be followed. The examples above signify the potential applicable law that could be applied if a legal dispute was raised in England.

This difficulty of determining the applicable law in unpermissioned blockchain technology has an additional layer 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 that can increase the traditional determination of applicable law.[123] However, as stated previously, liability is often limited by exchanges and DEXs and so this may not provide significant benefit to users who suffer losses in the exchange or DEX methods of interaction. Furthermore, the increased potential of determining the applicable law in the exchange or DEX methods of interaction, offers no help where the fault is in the execution of the blockchain on the peer-to-peer method. Nevertheless, English Courts in the *Ion Science*[124] and *Fetch.ai*[125] cases have indicated that they are willing to apply English Law where the claimant was domiciled in England.[126] Some exchanges even specify the applicable law in their terms and conditions.[127] Therefore, often the lex domicilii will prevail. Lex domicilli is defined as "the law of the domicile by which the rights of persons are sometimes governed."[128]

---

[117] (n115). 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

[118] For a brief discussion of how unpermissioned blockchain technology makes no reference to any hierarchy see, 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 July 2018, Page 104

[119] *Caparo Industries Plc* v *Dickman* [1990] 2 AC 605, Page 658 ('The Caparo test')

[120] *Robinson* (Appellant) v *Chief Constable of West Yorkshire Police* (Respondent) [2018] UKSC 4, Para 21

[121] Ibid, Para 27

[122] Ibid, Para 26

[123] (n42), Page 17

[124] *Ion Science Ltd* v *Persons Unknown and Others* (unreported) 21st December 2020 (Commercial Court)

[125] *Fetch.ai* v *Persons Unknown and Others* [2021] EWHC 2254 (Comm), 2021 WL 03605514

[126] Collyer Bristow, 'Financial Services Winter update 2021' (2nd December 2021) <https://collyerbristow.com/videos/financial-services-winter-update-2021/> Accessed 7th December 2021, Minutes 43-46

[127] Coinfalcon.com, 'Terms' <https://coinfalcon.com/en/terms> Accessed 23rd June 2020, (Jurisdiction and Applicable Law)

[128] Merriam-Webster Online dictionary, 'lex domicilii' <https://www.merriam-webster.com/dictionary/lex%20domicilii> Accessed 17th June 2020

The *Fetch.ai*[129] case also raises a further issue when considering jurisdictional complications. In that case, fraudsters managed to gain access to Fetch.ai's cryptocurrency accounts on the exchange Binance.[130] 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.[131] In the *Fetch.ai* case,[132] 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.[133] The Court in this case sided 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.[134]

This indicates 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.[135] The key issue here is that any injunctions to freeze assets globally and the effectiveness of such proceedings is heavily reliant on the cooperation of many parties both domestically and internationally, as well as the skill of investigators.[136] Even though English courts are highly respected,[137] there may be little practical benefit of an international asset freezing order if other jurisdictions do not uphold it.

For this paper, we will continue with a presumption that the lex domicilii will prevail. For example, an English based exchange, without stating otherwise, will settle disputes in the English Legal court system and English law will be applied in line with any contractual agreement. Although, due to the supranational nature of the technology and the potential for anonymity the determination of applicable law is more complex than courts applying English law to English exchanges. 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.

Jurisdictional law

Determining which legal jurisdiction can resolve disputes is a vital component of any agreement between two parties.[138] The reasons for selecting certain jurisdictions can differ. In most cases, it is a matter of convenience for both 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, there may not be a mention of these terms because there is no intention for legal rights to be exercised.

In theory, if a dispute was brought to the courts (discarding temporarily the issues of anonymity and other enforcement issues highlighted), then cases could be brought in any country.[139] It would ultimately be the discretion of the claimant to commence litigation wherever is more favourable for their circumstances as there is no express statement of which

---

[129] (n125)
[130] (n126), Minute 37
[131] Ibid
[132] (n125)
[133] (n126), Minutes 38-39
[134] 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 7th December 2021
[135] (n126), Minutes 45-47
[136] Ibid, Minutes 48-51
[137] Ibid, Minutes 49-51
[138] (n104), 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.
[139] (n83), Page 1392

jurisdictional law will apply. Additionally, because of the supranational possibilities with unpermissioned blockchain technology, it 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 that they may be.[140] Therefore, the user could bring the case in whichever jurisdiction is more convenient or even favourable to them.[141] This means that there is no jurisdictional certainty and ultimately it is left up to the decision of the user (if the exchange or DEX has not specified). This highlights the difficulty of determining jurisdictional law and the need for development of approaches to handle these disruptive technologies.

Similarly to applicable law, the use of exchanges and DEXs can 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.

As already alluded to, irrespective of jurisdictional complications, there is still the presence of the obstacle of anonymity. 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. As mentioned previously, these factors are difficult to resolve in a platform using unpermissioned blockchain technology, and so potentially more unique legal approaches may be required to deal with these unique obstacles.

Summary:

It has been highlighted that various difficulties exist for the resolution of disputes regarding faults within unpermissioned blockchain technology. The use of the technology has developed from the original peer-to-peer method to the inclusion of exchanges and DEXs and may develop further.[142] The landscape of these different methods is fundamentally distinct from one another and so we cannot assess unpermissioned blockchain technology holistically. Academic debate and regulatory decisions must consider these distinctions to provide a practical response. The peer-to-peer method, with cryptography and other security elements, seems to be sufficiently secure and may be referred to as immutable.[143] Although, it is not without risk due to the potential threat of theft of the private key[144] and the possibility of the 51% attack.[145] Furthermore, there have been forks within the peer-to-peer method such as Ethereum, which may create differing security concerns.

Whilst the peer-to-peer method can be regarded as immutable, the same is not true of the other methods of interaction such as the exchange and DEX methods. A significant number of users tend to interact with the cryptocurrencies using unpermissioned blockchain through an exchange or DEX. These methods potentially expose users to additional risks and greater focus must be had here from an academic and regulatory standpoint. The threat of ‘hacking’ is

[140] For a discussion of this very issue but in relation to smart contracts see (n19), Page 444
[141] This issue is heightened further with the use of VPN blockers as true user location/jurisdiction may also be problematic to determine.
[142] Syren Johnstone, *Rethinking the Regulation of Cryptoassets: Cryptographic Consensus Technology and the New Prospect* (Elgar Publishing 2021), Page 169
[143] (n17), Page 16
[144] (n71)
[145] (n72)

prevalent in both the exchange-based method and the DEX method.[146] Therefore, the method of interaction can significantly impact the level of risk that a user may be exposed to.

The presence of the intermediary 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 paper.[147] The methods of interaction with the technology are distinct from one another and so any legal approach must factor this in. It is suggested that the law will need to treat each method of interaction separately rather than attempting to provide a uniform legal approach irrespective of the method of interaction.

Furthermore, the potential for anonymity in unpermissioned blockchain technology exists and this provides the most significant obstacle from a legal standpoint.[148] 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.[149] Should further regulation of the conduct on the peer-to-peer method be sought by regulators, the issue of anonymity presents a key obstacle that must be considered and potentially mitigated. Otherwise, the practicality of the legal approach would be diminished.

The supranational nature of blockchain technology provides an additional obstacle for legal redress. An ideal solution would be in the form of a global convention to create a uniform legal approach and the pooling of resources. However, the likelihood of this is limited.[150] In the absence of a convention 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.[151] This provides an additional obstacle that must be considered when discussing the application of the law in this area.

Blockchain technology may have been praised for its novelty and uniqueness.[152] However, the same uniqueness can create further legal issues. Unpermissioned blockchain technology poses numerous legal issues that may be regarded as distinct 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 may be required to practically deal with the unique issues posed by unpermissioned blockchain technology.[153]

---

[146] Usman W Chohan, 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns' (2018) Discussion Paper Series: Notes on the 21st Century 1; 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 7th December 2021

[147] (n42), Page 17

[148] (n91)

[149] (n78)

[150] (n104)

[151] (n126), Minutes 45-51

[152] (n5)

[153] This is the subject of further research by me.