

11-6-2018

Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers

Jean Bacon

Microsoft Cloud Computing Research Centre

Johan David Michels

Microsoft Cloud Computing Research Centre

Christopher Millard

Microsoft Cloud Computing Research Centre

Jatinder Singh

Microsoft Cloud Computing Research Centre

Follow this and additional works at: <https://scholarship.richmond.edu/jolt>

Recommended Citation

Jean Bacon, Johan D. Michels, Christopher Millard & Jatinder Singh, *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers*, 25 Rich. J.L. & Tech 1 ().

Available at: <https://scholarship.richmond.edu/jolt/vol25/iss1/2>

This Article is brought to you for free and open access by the Law School Journals at UR Scholarship Repository. It has been accepted for inclusion in Richmond Journal of Law & Technology by an authorized editor of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.

**BLOCKCHAIN DEMYSTIFIED: A TECHNICAL AND LEGAL
INTRODUCTION TO DISTRIBUTED AND CENTRALISED
LEDGERS⁺**

Jean Bacon^{*}
Johan David Michels^{**}
Christopher Millard^{***}
Jatinder Singh^{****}

Cite as: Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers*, 25 RICH. J.L. & TECH., no. 1, 2018.

⁺ This paper has been produced by members of the Microsoft Cloud Computing Research Centre, a collaboration between the Cloud Legal Project, Centre for Commercial Law Studies, Queen Mary University of London and the Department of Computer Science and Technology, University of Cambridge. The authors are grateful to members of the MCCRC team and to attendees at the 4th Annual MCCRC Symposium (September 2017) for helpful comments and to Microsoft for the generous financial support that has made this project possible. We also acknowledge the financial support of the UK Engineering and Physical Sciences Research Council (EPSRC). Responsibility for views expressed, however, remains with the authors.

^{*} Professor Emerita of Distributed Systems, Department of Computer Science and Technology, University of Cambridge.

^{**} Researcher, Cloud Legal Project and Microsoft Cloud Computing Research Centre, both at the Centre for Commercial Law Studies, Queen Mary University of London.

^{***} Professor of Privacy and Information Law and Project Leader, Cloud Legal Project, Centre for Commercial Law Studies, Queen Mary University of London and Senior Counsel, Bristows LLP. Joint Director of the Microsoft Cloud Computing Research Centre.

^{****} Senior Research Fellow, Department of Computer Science and Technology, University of Cambridge.

ABSTRACT

This paper provides an introduction to blockchain technology and its legal implications. The paper consists of two parts. The first part looks at the technology behind the hype. It explains how blockchain technology works and can be deployed in various ways to create applications with different features, including open, distributed and closed, and centralised platforms. The second part analyses the technology's implications for several areas of law that will be relevant to companies and other organisations that seek to use blockchain technology, namely: contract law, data protection law, securities law, property law, intellectual property, and company law. The purpose of this paper is to help legal and other professional advisors understand blockchain technology and to alert users of blockchain technology to the current legal uncertainty and associated risks.

TABLE OF CONTENTS

I. INTRODUCTION	4
1.1 Blockchain Technology	5
1.2 Legal Analysis	8
II. THE TECHNOLOGY BEHIND THE HYPE	9
2. Core Components	9
2.1 Data Integrity	9
2.2 Identity Authentication.....	13
2.3 Summary	16
3. Trust and Control	16
3.1 Trustless Environments and Open, Distributed Platforms	18
3.2 Trusted Parties and Closed, Centralised Platforms.....	28
3.3 Governance and Control	33
4. Visibility and Identity	41
4.1 Visibility of the Record: Public and Private Platforms	41
4.2 Identity of Participants	43
5. Smart Contracts	45
III. BLOCKCHAIN AND THE LAW	49
6. Legal Analysis.....	49
6.1 Smart Contracts and Contract Law.....	50
6.2 Blockchain Data and the GDPR	58
6.3 Initial Coin Offerings and Securities Law	78
6.4 Digital Tokens and Property Law	84
6.5 Blockchain Databases and Intellectual Property Law.....	95
6.6 Digital Autonomous Organisations and Company Law.....	99
IV. CONCLUSIONS	101
7.1 Blockchain Technology	101
7.2 Blockchain and the Law	104

I. INTRODUCTION

[1] Excitement about blockchain and related technologies is soaring to new heights. The value of the two main cryptocurrencies, Bitcoin and Ethereum, has proved volatile with Bitcoin's price increasing twentyfold, from U.S. \$1,000 in January 2017 to almost U.S. \$20,000 in December 2017, before plummeting to around U.S. \$9,000 as of March 2018.¹ Initial Coin Offerings (ICOs) raised an estimated U.S. \$5.5 billion in 2017.² Organisations ranging from banks to charities publicly expressed their interest in using blockchain technology.³ This flurry of activity sparked responses by legislators and regulators, including securities regulators in the United States and the EU.⁴

¹ See *Bitcoin (USD) Price*, COINDESK, <https://www.coindesk.com/price/> (last visited Oct. 5, 2018) (change the date range in the chart to reflect January 1, 2017 as the start date and March 31, 2018 as the end date).

² See Ben McLannahan, *SEC Cyber Unit Eyes Initial Coin Offerings with Suspicion*, FIN. TIMES (Mar. 15, 2018), <https://www.ft.com/content/b797e1ac-1b04-11e8-aaca-4574d7dabfb6> [<https://perma.cc/7C94-XLSG>].

³ See, e.g., Due.com, *Are Banks Ready to Embrace Blockchain Technology?*, NASDAQ (June 5, 2017, 10:00:43 AM EDT), <https://www.nasdaq.com/article/are-banks-ready-to-embrace-blockchain-technology-cm798599> [<http://perma.cc/75B4-EV6J>]; Paul Lamb, *Transforming the Social Sector: Bitcoin and Blockchain for Good*, HUFFPOST, https://www.huffingtonpost.com/entry/transforming-the-social-sector-bitcoin-and-blockchain_us_59c169e3e4b0f96732cbc9c7 [<https://perma.cc/9FW5-TP7S>] (last updated Jan. 8, 2018).

⁴ See McLannahan, *supra* note 2; see also *ESMA Highlights ICO Risks for Investors and Firms*, EUR. SEC. & MKTS. AUTHORITY (Nov. 13, 2017), <https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms> [<https://perma.cc/49K7-6PM>].

[2] There are many tutorials and reports, and various books on blockchain.⁵ However, a lot of the existing material assumes that readers are familiar with the underpinning technologies. Further, some sources fail to distinguish between the core components of blockchain technology, and the various ways in which the technology can be applied. Finally, the terminology used to describe blockchain is often unclear or inconsistent. As a result, many discussions of blockchain are marred by misunderstandings and can leave audiences mystified.

[3] This paper aims to demystify blockchain for a non-expert audience. It consists of two parts. The first part is an introduction to blockchain technology. The second part explores blockchain's legal implications. It argues that understanding the different ways in which platforms can apply blockchain technology is often key to accurate legal analysis. As a result, there can be no one-size-fits-all legal response. Instead, this paper aims to help legislators, regulators, and lawyers understand blockchain technology, so they can tailor appropriate legal solutions to each use case. Moreover, the initial exploration of legal implications could help those considering the use of a blockchain solution in almost any context.

1.1 Blockchain Technology

[4] In our view, a blockchain is a type of database: a structured collection of information. In this paper, we use the term *blockchain* to refer to a specific type of database that uses certain cryptographic functions to achieve the requirements of data integrity and identity

⁵ See, e.g., ANDREAS M. ANTONOPOULOS, *MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES* (1st. ed 2014); ARVIND NARAYANAN ET AL., *BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION* (Princeton Univ. Press eds., 2016); ROGER WATTENHOFER, *THE SCIENCE OF BLOCKCHAIN* (Inverted Forest Publishing eds., 2016).

authentication, as set out in the table below. Since blockchains commonly track transactions, they are often referred to as *ledgers*.⁶

Table 1. Two Key Requirements of Blockchain Technology

No.	Requirement	Component	Purpose
1.	Data integrity	Hash functions	To create a persistent, tamper-evident record of relevant transactions.
2.	Identity authentication	Public key infrastructure	To authenticate the party or parties associated with each transaction.

[5] In Section 2, below, we explain how hash functions can be used to create a persistent, tamper-evident record of transactions.⁷ Then, we show how public key infrastructure (PKI) can authenticate the identity of the parties associated with those transactions.⁸

[6] We use the term distributed ledger technology (DLT) to refer to a ledger that is stored in a distributed manner across a peer-to-peer network. By this definition, a distributed ledger (DL) is also a blockchain if it uses a blockchain data structure to record transactions. However, a blockchain that is stored in a centralised manner is not a DL because it is not distributed.

[7] Cryptocurrencies, like Bitcoin and Ethereum, are the most well-known applications of blockchain technology and have shaped the public

⁶ See NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, DRAFT NISTIR 8202 BLOCKCHAIN TECHNOLOGY OVERVIEW (2018), at 15 [hereinafter NISTIR OVERVIEW].

⁷ See discussion *infra* Section 2.1.

⁸ See discussion *infra* Section 2.2.

perception of what *blockchain* is.⁹ However, the Bitcoin and Ethereum platforms were configured to meet specific requirements for creating a digital currency that anyone can access known as *open* or *permissionless* systems.¹⁰ They were intended to enable a so-called *trustless environment*, meaning the participants to a transaction need not trust each other.¹¹ These requirements shaped the ways in which early platforms applied blockchain technology, including with regard to public visibility and user pseudonymity.¹² Blockchains can be applied in a variety of ways to create platforms with different properties and features.¹³ As blockchain technology is adopted for purposes other than currencies, the early requirements may not necessarily be carried forward. For instance, some applications entail *closed* or *permissioned* systems where participation is limited to a certain group of approved users.¹⁴ In such cases, there is likely to be a higher level of trust among users, reducing the need for distributed storage and consensus protocols.¹⁵

⁹ See David Hollerith, *Survey Polls American Awareness of Cryptocurrencies and ICOs*, BITCOIN MAG. (Nov. 6, 2017, 2:53 PM EST), <https://bitcoinmagazine.com/articles/survey-polls-american-awareness-cryptocurrencies-and-icos/> [<https://perma.cc/SAG2-QKCM>].

¹⁰ See NISTIR OVERVIEW, *supra* note 6, at 38.

¹¹ See *id.* at 45.

¹² See Jean Bacon, Johan David Michels, Christopher Millard, & Jatinder Singh, *Blockchain Demystified 5* (Queen Mary University of London, School of Law Legal Studies Research Paper, No. 268/2017, 2017), <https://ssrn.com/abstract=3091218> [[https://perma.cc/5\(U6-9F65\)](https://perma.cc/5(U6-9F65))] (citing the requirements of early cryptocurrencies); Daniel Genkin, Dimitrios Papadopoulos, & Charalampos Papmanthou, *Privacy in Decentralized Cryptocurrencies*, 61 COMM. ACM, June 2018, at 78, 78, <https://cacm.acm.org/magazines/2018/6/228028-privacy-in-decentralized-cryptocurrencies/fulltext> [<https://perma.cc/7D4M-DTYS>] (discussing user pseudonymity).

¹³ See NISTIR OVERVIEW, *supra* note 6, at 40–44.

¹⁴ See *id.* at 36.

¹⁵ See discussion *infra* Section 3.2.

[8] In Sections 3 and 4, we explain how early platforms have applied blockchain technology in open, permissionless ways to create distributed ledgers. We then turn to closed, permissioned platforms and consider how these might differ in terms of their configuration and features, including centralised ledgers. Section 3 looks at the key issue of control over the blockchain. Section 4 considers the visibility of the blockchain record and user identity. Section 5 briefly outlines the role of smart contracts.

1.2 Legal Analysis

[9] Part Two explores blockchain technology's legal implications. In Section 6, we consider the legal implications of smart contracts, digital autonomous organisations, initial coin offerings, and digital tokens under contract law, data protection law, securities law, property law, intellectual property, and company law. In each area, we focus on legal issues raised by blockchain technology, as opposed to how blockchain technology can be used to improve compliance with legal requirements.

[10] We conclude that any particular blockchain-based platform may be more or less decentralised and more or less anonymous, based on application requirements and associated technical design decisions. These features in turn have significant legal implications, for instance with regard to the difficulty of reversing past transactions. This paper does not explore how blockchain transactions relate to real-world assets. While early applications tracked on-chain assets (i.e. digital tokens which exist only by virtue of the blockchain), some future applications will use tokens to reflect off-chain assets, including physical items, raising further legal complications.¹⁶

¹⁶ See Chris Reed, Umamahesh Sathyanarayan, Shuhui Ruan, & Justine Collins, *Beyond Bitcoin—Legal Impurities and Off-chain Assets*, 5–6 (Queen Mary University of London, School of Law Legal Studies Research Paper, No. 260/2017, 2017), <https://ssrn.com/abstract=3058945> [<https://perma.cc/C7EM-L4WL>].

II. THE TECHNOLOGY BEHIND THE HYPE

2. Core Components

2.1 Data Integrity

[11] Blockchain technology aims to create a persistent, tamper-evident record of relevant transactions.¹⁷ This section shows how hash functions can be used to create a tamper-evident data structure.

2.1.1 Hash Values Prove the Integrity of Data

[12] Hashing involves putting a data item (e.g. the contents of a document) through a *hash function*.¹⁸ This function creates a string of digits of a fixed length that are unique to the input data item.¹⁹ The output is called a *hash value*.²⁰ It is practically *impossible* for two different data items to hash to the same value (i.e. the probability of that occurring is extremely low).²¹

[13] As a result, hashing can be used to prove the integrity of the input data.²² If the original input is changed in any way—even by a single

¹⁷ See NISTIR OVERVIEW, *supra* note 6, at 1–2.

¹⁸ See DONALD E. KNUTH, THE ART OF COMPUTER PROGRAMMING (Addison Wesley Longman eds., 2d ed. 1998).

¹⁹ See *id.*

²⁰ See *id.*

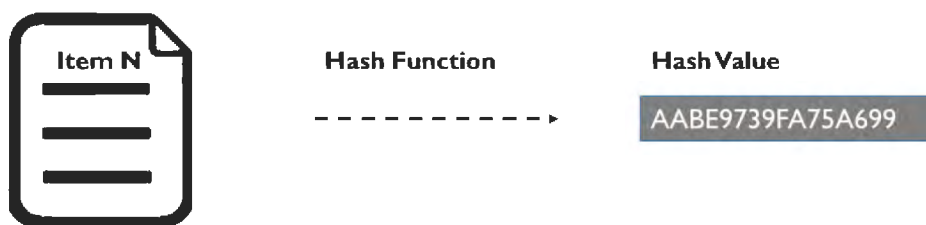
²¹ See Mohammad Peyravian et al., *On Probabilities of Hash Value Matches*, 17 COMPUTERS & SEC., 171, 171–73 (1998), http://www.mathcs.emory.edu/~whalen/Hash/Hash_Articles/On%20probabilities%20of%20hash%20value%20matches.pdf [<https://perma.cc/M23H-X6JA>].

²² See *Ensuring Data Integrity with Hash Codes*, MICROSOFT (Mar. 29, 2017), <https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes> [<https://perma.cc/ZJC9-JUSJ>].

character or space—the function will produce a totally unrelated hash value.²³ To prevent tampering, this requires the hash value—but not the data item itself—to be visible to external observers. If the hash value is unchanged, observers can be confident that the input data has not been tampered with.²⁴

Figure 1: A Hash Function That Outputs a 16-digit (8 byte, 64 bit) Hash Value

Item N hash = hash (Item N data)



[14] Hashing is *one-way*, in that it is not possible to recreate the original input from the hash value that the hash function outputs.²⁵ Hashing does not change or otherwise affect the input data item.²⁶ Unencrypted data, with the associated hash value, are readable by anyone with access to them.²⁷ In sum, the combination of a data item and its hash value is

²³ See NARAYANAN, *supra* note 5, at 12–15.

²⁴ See Kyriacos Pavlou & Richard T. Snodgrass, *Forensic Analysis of Database Tampering*, 33 ACM TRANSACTIONS ON DATABASE SYS. 109, 110 (2008), <https://www2.cs.arizona.edu/~rts/pubs/SIGMOD06.pdf> [<https://perma.cc/W552-TEJF>].

²⁵ See NISTIR OVERVIEW, *supra* note 6, at 12–13; see KNUTH, *supra* note 18.

²⁶ See BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C, § 2.4 (John Wiley et al. eds., 20th Anniversary ed., 2015) [hereinafter APPLIED CRYPTOGRAPHY] (discussing how the hash function merely takes an image of the input data and converts that image into a hash value).

²⁷ See *id.* §§ 8.4, 18.12.

tamper-evident, in that it would be evident to any observer if the data item were changed in any way.²⁸

2.1.2 Hash Pointers Create Tamper-Evident Data Chains

[15] Hash values can also be used to make a data structure of multiple data items tamper-evident, through *hash pointers*.²⁹ Hash pointers prove the integrity of a string of data items, including both their contents and their sequence.³⁰

[16] Hash pointers achieve this by linking a series of items together, as illustrated in Figure 2 below for Items 6–8.³¹ The data of each item is combined with the hash value of the previous item and put into a hash function.³² This generates that item’s hash value, which is then included in the next item.³³ For example, the hash value of Item 8 is based on both Data 8 and the hash of Item 7. Item 7 contains Data 7 and the hash of Item 6, and so on, back to the start of the chain.

²⁸ *See id.* § 8.4 (arguing that it is very difficult to tamper with and substitute keys without another person noticing); *see also* NISTIR OVERVIEW, *supra* note 6, at 52 (describing a tamperproof hash chain).

²⁹ *See* NISTIR OVERVIEW, *supra* note 6, at 19–23.

³⁰ *See id.*

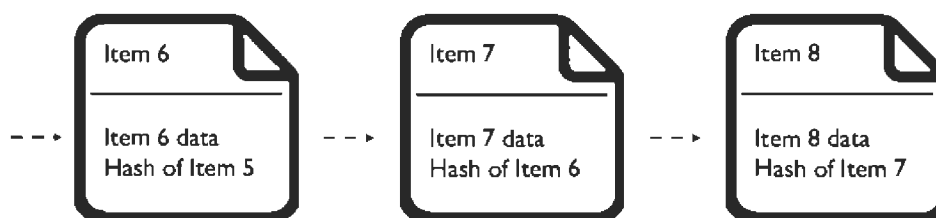
³¹ *See id.*

³² *See id.*

³³ *See id.*

Figure 2. A Tamper-evident Chain of Items Using Hash Pointers

Item N hash = hash (Item N data, Item N-1 hash)



[17] This results in a tamper-evident data chain. The data of Item 7 cannot be changed without changing its hash value. Any attempt to change the values of Item 7 and *re-hash* it would break the link between the items, since the hash of Item 7 is recorded in Item 8. Provided an external observer can view the hash pointers, they can spot any tampering. So, if a (fraudulent) change were to be made in the data of Item 7, all subsequent blocks in the chain would have to be re-hashed to rebuild the chain.

2.1.3 Blockchains Group Transactions into ‘Blocks’ in a ‘Chain’

[18] Blockchains record large numbers of transactions.³⁴ For efficiency reasons, they achieve this by grouping individual transaction records together into a block, and chaining blocks together using hash pointers, instead of merely linking single data items.³⁵

[19] A block consists of two parts. The *block body* contains the transactions that the block records.³⁶ The *block header* includes the hash

³⁴ See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 2, <https://bitcoin.org/bitcoin.pdf> [<https://perma.cc/Y9QJ-UD9A>] (explaining the process of how transactions are verified by a chain of ownership).

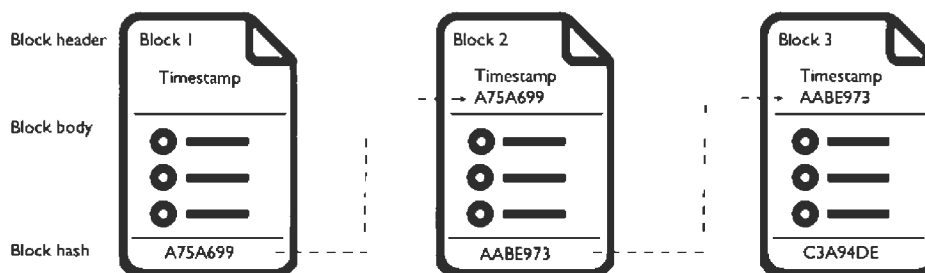
³⁵ See NISTIR OVERVIEW, *supra* note 6, at 23.

³⁶ See *id.* at 19–23; see also Minhaj Ahmad Khan & Khaled Salah, *IoT Security: Review, Blockchain Solutions, and Open Challenges*, 82 FUTURE GENERATION COMPUTER SYS. 395, 405 (2018).

of the previous block and some metadata such as a timestamp.³⁷ Blocks are hashed as a whole, i.e. the header and the body are used as input data for the hash function.³⁸ Thus, a block's hash value is created from data that includes the hash of the previous block.³⁹ Blocks are chained using these block hash pointers, creating a *blockchain*, as shown in Figure 3.⁴⁰

Figure 3. A Simple Blockchain Representation Showing Three Chained Blocks

Block N hash = hash (Block N header, Block N body)



In practice, for scalability and to limit access latency, a more general 'Merkle Tree' structure is used to record the transactions within each block.⁴¹

2.2 Identity Authentication

[20] To record a transaction or other data item securely, blockchain technology needs to authenticate the relevant parties, before storing it in a

³⁷ *See id.*

³⁸ *See id.*

³⁹ *See id.*

⁴⁰ *See id.* Figure 3 does not represent any particular platform's block header in detail and is intended as an example.

⁴¹ *See Nakamoto, supra* note 34, at 4.

tamper-evident database.⁴² Otherwise, an attacker could simply pose as another party and propose new transactions, such as sending another user's Bitcoins to an address they control. This section explains how blockchain technology uses public key infrastructure to authenticate users' identities and ward off such attacks.

[21] Public key infrastructure (PKI) allows users to generate a key pair consisting of a public and a private key to sign a data item, and to validate whether a digital signature is correct.⁴³ Data encrypted with the public key can only be decrypted using the private key and vice versa.⁴⁴ If a certain set of data can be decrypted with the public key, this proves the data was encrypted by, and therefore came from, the holder of the private key.⁴⁵

[22] As the names imply, users must never reveal their private keys, since anyone who knows a private key can masquerade as its owner.⁴⁶ Private keys should not be transmitted, even when encrypted.⁴⁷ Conversely, the public key is published to represent the individual or

⁴² See Steve Olshansky et al., *Do Blockchains Have Anything to Offer Identity*, INTERNET SOCIETY (Mar. 7, 2018), <https://www.internetsociety.org/resources/doc/2018/blockchain-identity/> [<https://perma.cc/CZQ4-N5KH>].

⁴³ See NISTIR OVERVIEW, *supra* note 6, at 13–14; see *Public Key Infrastructure*, MICROSOFT (May 30, 2018), <https://docs.microsoft.com/en-us/windows/desktop/seccertenroll/public-key-infrastructure> [<https://perma.cc/DMU7-SDVZ>].

⁴⁴ See SCHNEIER, *supra* note 26, § 2.7 (illustrating how two users can send and verify encrypted messages).

⁴⁵ See *id.*

⁴⁶ See NISTIR OVERVIEW, *supra* note 6, at 46.

⁴⁷ See *Public Key Cryptography*, IBM KNOWLEDGE CENTER, https://www.ibm.com/support/knowledgecenter/en/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm [<https://perma.cc/DJG4-3HGP>] (noting that the sharing of “secret keys makes them vulnerable to theft”).

entity holding the corresponding private key.⁴⁸ PKI can be used to create digital signatures, which establish that a transaction emanated from a certain user.⁴⁹ To sign a data item, the sender encrypts the data with their private key.⁵⁰ If the public key can be used to decrypt the data, this proves that the sender held the private key.⁵¹

[23] With blockchain, the private key is used to encrypt the transaction record.⁵² This effectively establishes that the transaction originated with the associated party. Either the owner of the corresponding private key must have signed the data, or the key has been compromised by theft or sharing. Transaction records are signed before being included in blocks.⁵³

[24] Each party's private key is their means of access to the blockchain platform.⁵⁴ If they lose their private key, the platform can no longer authenticate their identity and will deny them access.⁵⁵ Thus, if a user loses their Bitcoin private key, they can no longer access any associated coins.

⁴⁸ *See id.* (noting that the public key is distributed so that users may encrypt messages to the person holding the corresponding private key).

⁴⁹ *See* NISTIR OVERVIEW, *supra* note 6, at 46.

⁵⁰ *See id.* at 13–15.

⁵¹ *See id.*

⁵² *See id.*

⁵³ *See id.*

⁵⁴ *See* NISTIR OVERVIEW, *supra* note 6, at 14–15.

⁵⁵ *See* Matthew Sparkes, *The £625m Lost Forever—The Phenomenon of Disappearing Bitcoins*, TELEGRAPH, (Jan. 23, 2015, 7:00 AM), <https://www.telegraph.co.uk/technology/news/11362827/The-625m-lost-forever-the-phenomenon-of-disappearing-Bitcoins.html> [<https://perma.cc/D2F7-WEJD>].

2.3 Summary

[25] In sum, hash functions can be used to generate hash pointers that link blocks of transactions together in a chain. The hash pointers establish the integrity of the data within each block, as well as the order of the blocks, thereby creating a tamper-evident data structure. For example, Bitcoin generates hash pointers using Secure Hash Algorithm 256 (SHA-256), a well-known hash function that generates a 256-bit (or 32-byte) hash.⁵⁶

[26] A private key can be used to establish an individual's identity through a digital signature.⁵⁷ Blockchains combine private keys and hash functions to create a long-term, tamper-evident record of transactions between parties with verified identities.⁵⁸ However, the intended long-term storage of blockchain records raises the issue of whether current encryption schemes will continue to be sufficient. Quantum computing may present a challenge to encryption in the long term.

3. Trust and Control

[27] This section covers a key question for each application of blockchain technology, namely: who will control the blockchain? This can be split into three sub-questions: (i) who stores a copy of the current version of the blockchain; (ii) who can add new blocks to it, and (iii) who controls how the system works?

[28] As set out above, the use of a blockchain should give users confidence in a tamper-evident ledger of their transactions. Further, users should be confident that nobody can transfer their assets without access to their private key. However, using a blockchain does not in itself prevent

⁵⁶ See ANTONOPOULOS, *supra* note 5, at ch. 7.

⁵⁷ See NISTIR OVERVIEW, *supra* note 6, at 14, 46.

⁵⁸ See *id.*

tampering by whoever controls the ledger.⁵⁹ For example, an ill-intentioned record-keeper could potentially change transactions in past blocks and then re-hash all the blocks up to the present block, so that the new hash pointers link the blocks. Thus, in a system where visibility and control over the ledger are centralised in the hands of a single party, users need to trust this party not to tamper with the ledger.

[29] Early cryptocurrencies seek to provide a trustless environment.⁶⁰ Instead of centralising control, they allow anyone to store a local copy of the blockchain and propose new blocks for inclusion.⁶¹ To achieve this, they rely on a network of *nodes* to store copies across a peer-to-peer network and *miners* to propose new blocks, as explained in Section 3.1 below.⁶² We use Bitcoin as an example to illustrate the workings of an open, distributed platform.

[30] In contrast, future applications of the technology may operate in environments where there is a degree of trust. As a result, future platforms may feature either a single entity, known as a ‘Trusted Third Party’ or TTP, or a small group of participants that operate the blockchain. Section 3.2 considers how future, centralised platforms may differ from early cryptocurrencies. Finally, Section 3.3 covers issues of blockchain governance and control, including changes to the software and the possibility of reversing past transactions.

⁵⁹ *See id.* at 36–37.

⁶⁰ *See* Nakamoto, *supra* note 34, at 1–2 (describing a system in which two parties can transact directly without a trusted third party using a distributed, time-stamped system).

⁶¹ *See id.* at 3.

⁶² *See* discussion *infra* Section 3.1.

3.1 Trustless Environments and Open, Distributed Platforms

3.1.1 Users: Permissionless Access

[31] Early cryptocurrency platforms involve three overlapping groups: users, nodes, and miners.⁶³ Users participate in the platform by buying and selling coins like Bitcoin or Ether. To participate, they run open source code on their local hardware.⁶⁴ This software broadcasts the users' required transactions onto the network, to be incorporated into blocks by miners.⁶⁵ In Bitcoin, the pool of transactions waiting to be confirmed is called the *mempool*.⁶⁶

[32] In terms of access, early cryptocurrencies are open or permissionless at the user level.⁶⁷ For example, in Bitcoin, anybody can generate a public private key pair and a Bitcoin address via their open source software.⁶⁸ Alternatively, they can join a software wallet service online that generates the key pair for them.⁶⁹ To start trading, users can

⁶³ See NISTIR OVERVIEW, *supra* note 6, at 15–25.

⁶⁴ See *How Do Bitcoin Transactions Work?*, COINDESK (Jan. 29, 2018), <https://www.coindesk.com/information/how-do-bitcoin-transactions-work/> [<https://perma.cc/CC8Q-VH2U>].

⁶⁵ See *id.*

⁶⁶ See, e.g., *Mempool Size*, BLOCKCHAIN.COM, <https://blockchain.info/charts/mempool-size> [<https://perma.cc/3BF3-BTBM>].

⁶⁷ See NISTIR OVERVIEW, *supra* note 6, at 38–40.

⁶⁸ See *id.* at 14; Noelle Acheson, *How to Store Your Bitcoin*, COINDESK (Jan. 20, 2018), <https://www.coindesk.com/information/how-to-store-your-bitcoins/> [<https://perma.cc/ZKH3-7D89>] [hereinafter Acheson, *How to Store Bitcoin*] (noting that free software can be used to install a wallet, and how the original software wallet was Bitcoin Core).

⁶⁹ See, e.g., COINBASE.COM, <https://wallet.coinbase.com> [<https://perma.cc/H8Y5-BDBY>]; BLOCKCHAIN.COM, <https://login.blockchain.com/#/signup> (last visited Sept. 15, 2018) (allowing users to join an online wallet service).

buy Bitcoin from online exchanges, or by finding other users to trade Bitcoin in person.⁷⁰ However, using intermediary services such as wallets or exchanges requires a level of trust from participants, since they store copies of the user's private key.⁷¹ While the Bitcoin system itself has not been hacked, several exchanges have been, resulting in substantial losses.⁷²

3.1.2 Nodes: Storage and Validation

[33] Nodes store a local copy of the blockchain.⁷³ *Full* nodes store a copy of the entire blockchain, while *light* nodes hold only a subset of the blockchain in order to verify transactions.⁷⁴ The early applications of blockchain technology are also *open* or *permissionless* at the node level. Anybody can become a node by downloading and running the relevant software and storing the blockchain archive.⁷⁵ In practice, only a subset of users will do so, since this requires significant bandwidth and storage space.⁷⁶ As of March 2018, running a full node requires 145GB of free

⁷⁰ See generally LOCALBITCOINS.COM, <https://localbitcoins.com> [<https://perma.cc/KVH8-X7ZL>] (providing users an online form to buy and sell Bitcoin).

⁷¹ See Kevin D. Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, BERKELEY TECH. L.J. (forthcoming 2018) (manuscript at 27), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844409 [<https://perma.cc/2DUM-KHMZ>] (comparing the trust users extend to wallet service providers storing their private cryptographic keys to the trust a consumer extends to a bank).

⁷² See *id.* at manuscript 27–28 (describing several incidents of hacking).

⁷³ See NISTIR OVERVIEW, *supra* note 6, at 23–24.

⁷⁴ See *id.* (describing the differences between *full* and *light* node).

⁷⁵ See *id.* at 36–40.

⁷⁶ See *Running a Full Node*, BITCOINCORE, <https://bitcoin.org/en/full-node#what-is-a-full-node> [<https://perma.cc/MK3J-6S8G>].

disk space.⁷⁷ There were over 10,000 nodes running on the Bitcoin core network as of March 2018.⁷⁸

[34] Nodes discover and maintain connections with other nodes across a P2P network.⁷⁹ When they receive a new block from another node on the network, they check that it is valid.⁸⁰ This includes a check to prevent users spending the same coin twice, known as double-spending.⁸¹ They do so by checking the proposed transaction against a list of previous, unspent transaction outputs, known as the UTXO database.⁸² If the block is valid, the node adds it to their local copy of the blockchain and broadcasts it to other nodes on the network.⁸³

3.1.3 Miners: Distributed Control Over New Blocks

[35] Miners assemble transactions into blocks and broadcast those blocks to nodes across the P2P network, so the nodes can append the new block to their local copies⁸⁴ Miners are rewarded for adding new blocks

⁷⁷ *See id.*

⁷⁸ *See Bitcoin Core Nodes (historical)*, COIN DANCE, <https://coin.dance/nodes> [<https://perma.cc/25TM-WRFL>].

⁷⁹ *See NISTIR OVERVIEW*, *supra* note 6, at 23–25.

⁸⁰ *See id.* at 26–29.

⁸¹ *Double Spend*, BITCOIN, <https://bitcoin.org/en/glossary/double-spend> [<https://perma.cc/R476-L6RX>].

⁸² *See* Gavin Andresen, *UTXO uh-oh...*, SVBTLE BLOG (May 8, 2015), <http://gavinandresen.ninja/utxo-uhoh> [<https://perma.cc/XN8Y-SNMK>] A transaction output is the result of a transaction, transferring an amount of coin that is not yet spent to a new address. The transaction giving ownership to the payer is removed from the UTXO and the transaction giving the currency to the payee is added to the UTXO. All inputs to a transaction must be in this database for the transaction to be valid.

⁸³ *See NISTIR OVERVIEW*, *supra* note 6, at 23–25.

⁸⁴ *See id.* at 26–28.

with newly minted crypto-coins, as well as any transaction fees users have offered.⁸⁵ Bitcoin and Ethereum are open or permissionless at the miner level.⁸⁶ Any user can become a miner by running mining software on their local machine.⁸⁷ Thus, these early applications were designed to be open or permissionless on three levels, as set out in the table below.

Table 2. Bitcoin: An Open/Permissionless Application of Blockchain Technology

No.	Group	Function	Permission
i.	Users	Propose new transactions	Open: Anyone can join the network and send and receive Bitcoin.
ii.	Nodes	Store copies of the DL	Open: Anyone can download the software and run a Bitcoin node.
iii.	Miners	Propose new blocks	Open: Anyone can mine new blocks and broadcast them to the P2P network

3.1.4 Distributed Storage and Consensus Protocols

[36] Allowing anyone to operate a node means the blockchain can be stored in a distributed manner, i.e. as a Distributed Ledger or DL.⁸⁸ Storing a blockchain in such a way has three main advantages. First, it protects data from tampering by any single centralised party.⁸⁹ Second, a DL may be less vulnerable to attack since there is no single *master copy* of

⁸⁵ When a user signs a Bitcoin transaction, they can offer *transaction fees* in return for priority processing of their transactions. *See* Nakamoto, *supra* note 34, at 4.

⁸⁶ *See* NISTIR OVERVIEW, *supra* note 6, at 26–28.

⁸⁷ *See id.*

⁸⁸ *See id.* at 38.

⁸⁹ *See id.* at 36.

the ledger to target.⁹⁰ An attacker would instead have to make changes to a number of copies across the network. Finally, a DL is resilient, since there is no single point of failure to target with a denial of service (DoS) attack.⁹¹ Even if several nodes failed, the network would still continue to function.

[37] However, the major challenge for a DL is ensuring that all of the nodes hold a consistent and up-to-date copy of the blockchain and that participant/system behaviour is valid and appropriate.⁹² In blockchain terms, the nodes must achieve *consensus*.⁹³ *Full nodes* start by downloading the latest version of the ledger.⁹⁴ Thus, to achieve consensus, the system needs to ensure that each node adds the same new blocks to their local copy.⁹⁵ To this end, all nodes must follow the same rules for deciding when to add a new block.⁹⁶ These rules are called a consensus protocol, which is embedded in the software each node runs.⁹⁷ In an open, permissionless application, there may be thousands of widely distributed nodes holding copies. Therefore, these distributed consensus protocols cannot agree on new blocks one block at a time, as in conventional

⁹⁰ See Olivier Boireau, *Securing the Blockchain Against Hackers*, 2018 NETWORK SECURITY 8, 8–10 (2018).

⁹¹ See NISTIR OVERVIEW, *supra* note 6, at 9.

⁹² See *id.* at 26.

⁹³ See Nakamoto, *supra* note 34, at 8 (noting that nodes “vote with their CPU power” to accept and validate new blocks).

⁹⁴ See NISTIR OVERVIEW, *supra* note 6, at 23–24.

⁹⁵ See *id.*

⁹⁶ See *id.*

⁹⁷ See *id.* at 26.

consensus protocols.⁹⁸ Instead, they build up chains of blocks as they receive them.

[38] In order for nodes to accept their blocks, miners need to generate new blocks that accord with the consensus protocol.⁹⁹ Since anyone can join as a miner or node, the platform needs safeguards against malicious actors who try to take control of the ledger. If starting nodes and mining new blocks were costless, an attacker could flood the system with new nodes and newly mined blocks, in what is known as a *Sybil* attack.¹⁰⁰ To defend against this, early cryptocurrencies make mining new blocks costly, by requiring *proof of work*.¹⁰¹

i. Proof of Work

[39] The consensus protocol of Bitcoin and Ethereum requires miners to demonstrate proof of work (PoW) for each new block.¹⁰² To do so, each miner must find the answer to a computationally difficult *puzzle*.¹⁰³ Solving the puzzle can be seen as a demonstration of good faith, since it requires the miner to invest resources, CPU power and electricity, into

⁹⁸ See, e.g., Marko Vukolic, *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*, 9591 LECTURE NOTES COMPUTER SCI. 112 (2016) (discussing consensus protocols used by Bitcoin).

⁹⁹ See NISTIR OVERVIEW, *supra* note 6, at 26.

¹⁰⁰ See John Douceur, *The Sybil Attack*, in PEER-TO-PEER SYSTEMS 251, 252 (Peter Druschel et al. eds., 2002); see also Vukolic *supra* note 98, at 113.

¹⁰¹ See Nakamoto, *supra* note 34, at 3.

¹⁰² See NISTIR OVERVIEW, *supra* note 6, at 26–28.

¹⁰³ See *id.*

updating the ledger.¹⁰⁴ Nodes will only accept blocks that contain the solution to the puzzle.¹⁰⁵

[40] The puzzle works using hash functions.¹⁰⁶ As set out in Section 0, the header and body of a block are run through a hash function to generate that block's hash value.¹⁰⁷ To mine a valid new Bitcoin block, the hash value of that block must achieve a particular pattern, namely it must start with a certain number of zeros.¹⁰⁸ To create a valid block, a miner must add a random number, known as a *nonce*, to the header of the block such that the resulting hash value fits the pattern.¹⁰⁹ Miners solve this puzzle by trial-and-error, iterating through different nonces until the hash value has the required number of leading zeros.¹¹⁰ The higher the number of zeros required, the harder the puzzle.

[41] The more computational resources—CPU power—a miner devotes to solving the problem, the more likely they will solve it first.¹¹¹ In practice, professional miners use dedicated hardware, known as Application Specific Integrated Circuits (ASICs), and base themselves

¹⁰⁴ *See id.*

¹⁰⁵ *See id.*

¹⁰⁶ *See id.*

¹⁰⁷ *See* discussion *supra* Section 2.1.3.

¹⁰⁸ *See* Nakamoto, *supra* note 34, at 3.

¹⁰⁹ *See* NISTIR OVERVIEW, *supra* note 6, at 27; *see also* Vitalik Buterin, *A Next Generation Smart Contract & Decentralized Application Platform*, ETHEREUM WHITE PAPER, 6–7, [hereinafter Buterin, ETHEREUM WHITE PAPER] http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [https://perma.cc/VY99-CDUJ].

¹¹⁰ *See* NISTIR OVERVIEW, *supra* note 6, at 27.

¹¹¹ *See id.* at 28.

near sources of cheap electricity to increase their efficiency in mining Bitcoin.¹¹²

[42] The puzzle is difficult to solve, but easy to verify.¹¹³ This means that when a successful miner broadcasts a block with the solution to other nodes, they can easily check that the miner has solved it, by rehashing the block containing the miner's nonce.¹¹⁴ The nodes then propagate the valid block across the peer-to-peer network.¹¹⁵

[43] The difficulty of the puzzle and the amount of computational resource devoted to solving it determine the frequency of new blocks.¹¹⁶ The Bitcoin protocol dynamically adjusts the difficulty of the puzzle, to ensure that a new block is added every ten minutes, on average.¹¹⁷

[44] Although it enhances security, PoW uses large amounts of energy. All miners expend energy trying to solve the puzzle, but only one of the miners will successfully create a new block. Researchers have estimated that Bitcoin mining consumes 100–500 MW per day, or 3–16 PJ per year. This is similar to the yearly energy expenditure of c. 200,000-1.2m EU

¹¹² See Evelyn Cheng, *Bitcoin 'Mining' Goes from Enthusiasts to Giant Enterprises as Digital Currencies Surge*, CNBC (Aug. 1, 2017, 3:44 PM ET), <https://www.cnbc.com/2017/08/01/bitcoin-mining-goes-from-enthusiasts-to-giant-enterprises.html> [<https://perma.cc/5Z6Q-TG9F>].

¹¹³ See NISTIR OVERVIEW, *supra* note 6, at 28.

¹¹⁴ See *id.*

¹¹⁵ See *id.*

¹¹⁶ See Nakamoto, *supra* note 34, at 3.

¹¹⁷ See *id.* at 3; see also Buterin, ETHEREUM WHITE PAPER, *supra* note 109, at 6 (achieving consensus).

households.¹¹⁸ A single Bitcoin transaction requires an estimated 200kWh of energy, compared to around 0.01kWh per Visa transaction.¹¹⁹ To reduce the costs of achieving consensus, Ethereum is considering moving to a consensus protocol that combines proof of stake and sharding, i.e. partitioning a large database into many smaller parts.¹²⁰

ii. Attacking a PoW Blockchain

[45] As set out in Section 2.3 above, DLs have strong security mechanisms. For instance, regardless of how much hash power an attacker has, they cannot propose new transactions using another user's Bitcoins, since they do not have access to that user's private key.¹²¹ Nor can they spend the same coin twice in new transactions, since nodes would not verify those payments.¹²²

[46] Instead, to attack a DL that uses PoW, the attacker must gather more computational power than the rest of the network combined.¹²³ This is called a *51% attack*, since the attacker must control more than 51% of

¹¹⁸ See *Average Electricity Consumption Per Electrified Household*, WORLD ENERGY COUNCIL, <https://wec-indicators.enerdata.net/household-electricity-use.html#/primary-energy-intensity-adjusted-EU.html>, [<https://perma.cc/7B9Q-GPNQ>] (last updated May, 2016).

¹¹⁹ See *Why Bitcoin Transactions Are More Expensive Than You Think*, ING (Oct. 13, 2017), <https://think.ing.com/opinions/why-bitcoin-transactions-are-more-expensive-than-you-think/> [<https://perma.cc/XQ4E-L5YX>].

¹²⁰ See Vitalik Buterin, *Ethereum 2.0 Mauve Paper* (Sept. 15, 2018), [hereinafter Buterin, *2.0 Mauve Paper*] <https://cdn.hackaday.io/files/10879465447136/Mauve%20Paper%20Vitalik.pdf> [<https://perma.cc/Z86H-LDMH>]; see also NISTIR OVERVIEW, *supra* note 6, at 29

¹²¹ See Nakamoto, *supra* note 34, at 6.

¹²² See *id.* at 8.

¹²³ See *id.* at 1.

the hashing power in the system.¹²⁴ The attacker would be likely to consistently solve PoW first and thus, control the addition of new blocks.¹²⁵

[47] As a result, the attacker would not only consistently reap the mining rewards but could also reject blocks containing certain transactions in order to obtain benefit. In addition, an attacker controlling 51% of the hashing power could scam other users through a so-called *double-spending* attack.¹²⁶

[48] A single attacker would have to spend significant resources in order to obtain 51% hashing power. However, in practice, many Bitcoin miners work together as part of large, centrally operated *mining pools*.¹²⁷ Since the PoW problem is easy to partition, miners in these pools try to solve the puzzle independently and in parallel, by working on separate parts of the possible solution, but agree to share any earnings from mining blocks with others in the pool.¹²⁸ These pools concentrate hashing power and could be used for a 51% attack.¹²⁹ In 2015, some of the largest Bitcoin mining pools voluntarily split into smaller pools because the top two pools

¹²⁴ See Buterin, ETHEREUM WHITE PAPER, *supra* note 109, at 8.

¹²⁵ See Ittay Eyal & Emin Gun Sirer, *Majority is Not Enough: Bitcoin Mining is Vulnerable*, CORNELL U. LIBR. (Nov. 15, 2013), <https://arxiv.org/pdf/1311.0243.pdf> [<https://perma.cc/4LZ4-TEUD>].

¹²⁶ *See id.*

¹²⁷ *See* NISTIR OVERVIEW, *supra* note 6, at 28

¹²⁸ *See* Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP. 213, 222 (2015).

¹²⁹ *See* Primavera De Filippi & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure*, 5 INTERNET POL'Y REV. 1, 10–11 (2016).

held a majority of the CPU power.¹³⁰ As of March 2018, the largest Bitcoin mining pool (BTC.com) had 25% of the network's hash power.¹³¹

[49] That said, even if miners have the ability to engage in a 51% attack, they may not have the incentive to do so.¹³² Miners have an economic interest in maintaining high Bitcoin prices.¹³³ They are paid in Bitcoin for their mining and many have invested in dedicated hardware to support the currency.¹³⁴ A successful attack on Bitcoin would reduce its value, thereby jeopardising their ability to generate returns on their investment.¹³⁵ Nonetheless, the system remains vulnerable to a politically motivated 51% attack, for instance from a government commandeering one or more of the big mining pools.¹³⁶

3.2 Trusted Parties and Closed, Centralised Platforms

[50] Above, we have seen how early cryptocurrencies were designed to operate as open, permissionless platforms in trustless environments. As a result, they feature distributed storage and adding of new blocks managed

¹³⁰ See Larissa Lee, *New Kids on the Blockchain: How Bitcoin's New Technology Could Reinvent the Stock Market*, 12 HASTINGS BUS. L.J. 81, 107 (2016).

¹³¹ See *Bitcoin Hashrate Distribution*, BLOCKCHAIN, <https://blockchain.info/pools?timespan=24hrs> [<https://perma.cc/6WJ5-MGNX>].

¹³² See Nakamoto, *supra* note 34, at 4.

¹³³ See NISTIR OVERVIEW, *supra* note 6, at 44.

¹³⁴ See Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 861–63 (2015).

¹³⁵ See *id.*

¹³⁶ See *id.* at 863.

by complicated consensus protocols and resource-intensive mining to ensure that no single party controls the addition of new blocks.¹³⁷

[51] However, blockchain-based platforms need not all operate in trustless environments.¹³⁸ Instead, they may avoid costly consensus protocols by re-introducing trusted intermediaries that control the blockchain by storing copies, i.e. acting as nodes, and determining which new blocks are added, i.e. acting as miners. Having fewer miners also allows less costly conventional one-block-at-a-time consensus protocols to be used. Such systems are closed or permissioned at the level of nodes or miners, since storage and mining is limited to certain parties.¹³⁹ The result is a more centralised platform compared to the open, distributed platforms discussed above.

[52] Such solutions require a level of trust from users, either in a single centralised trusted third party (TTP) or in a small number of trusted nodes.¹⁴⁰ Closed, permissioned systems can offer better transparency and safeguards as regards data integrity compared to traditional databases and may themselves inspire trust, since parties can limit participation to keep malicious actors off the platform.¹⁴¹

[53] In many instances, consumers may prove willing to trust reputable companies and citizens may trust government agencies with centralised

¹³⁷ See generally Nakamoto, *supra* note 34 (discussing the structure of Bitcoin).

¹³⁸ See Vitalik Buterin, *On Public and Private Blockchains*, ETHEREUM: BLOG (Aug. 6, 2017), [hereinafter Buterin, *Public and Private Blockchain*] <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> [https://perma.cc/38QR-GRBM].

¹³⁹ See *id.*

¹⁴⁰ See *id.*

¹⁴¹ See *id.*

blockchain management.¹⁴² After all, they currently trust many centralised record-keepers to maintain accurate records, without the use of blockchains. For example, users currently trust Twitter not to change their past tweets. If tweets were stored on a blockchain, they would be tamper-evident. However, Twitter did not need a blockchain to gain users' trust, since users understand that tampering with past tweets would damage the company's reputation. This gives it a strong incentive to refrain from doing so. Users may similarly prove willing to trust reputable operators of closed, permissioned blockchain platforms.

[54] In terms of access, such centralised blockchain models can be open, permissionless at the user level—meaning anyone can join—or be closed, permissioned systems, access to which is limited to certain users.¹⁴³ For instance, a centralised blockchain operator can limit access only to users who have been through a vetting process.¹⁴⁴ We look at two models for closed, permissioned systems below.

3.2.1 A Centralised TTP Model

[55] Governments are exploring the use of blockchain for large, centrally managed databases, such as land registers.¹⁴⁵ Provided citizens are willing to trust their government, such a blockchain need not be stored at multiple nodes across a P2P network. Instead, it could be stored centrally with a government agency, such as the land registry, acting as a

¹⁴² See Izabella Kaminska, *Blockchain's Governance Paradox*, FIN. TIMES ALPHAVILLE (June 14, 2017, 5:50 PM), <https://ftalphaville.ft.com/2017/06/14/2190149/blockchains-governance-paradox/> [<https://perma.cc/5BFD-2TDG>].

¹⁴³ See Buterin, *Public and Private Blockchain*, *supra* note 138.

¹⁴⁴ See *id.*

¹⁴⁵ See, e.g., Stan Higgins, *UK Land Registry Plans to Test Blockchain in Digital Push*, COINDESK (May 12, 2017, 11:00 UTC), <https://www.coindesk.com/uk-land-registry-plans-test-blockchain-digital-push/> [<https://perma.cc/8RVU-QYN8>].

TTP.¹⁴⁶ The blockchain is publicly visible; this would increase the transparency of the registry's record-keeping, without requiring distributed storage.

[56] Estonia is often considered a pioneer in the use of blockchain technology.¹⁴⁷ Since Estonian independence in 1991, citizens have been issued a proof of identity via a PKI-based identity card.¹⁴⁸ Since 2012, blockchain-like approaches have been used to assist in maintaining the integrity of data and transactions regarding national health, judicial, legislative, and other public services.¹⁴⁹ A small number of dedicated nodes are involved in agreeing on the blocks in the ledger, with a view to checking that the constituent system components are operating correctly.

[57] To bolster trust in a TTP-based system, archival copies of the DL could be stored at independent nodes, such as with an Ombudsman. Any tampering by the record-keeper would then be evident through comparison with the independently-stored copies. Users would still need to trust the TTP and independent archival nodes not to collude against their interests.

¹⁴⁶ See Buterin, *Public and Private Blockchain*, *supra* note 138.

¹⁴⁷ See Colin Adams, *Estonia, A Blockchain Model for Other Countries?*, INVEST IN BLOCKCHAIN (Jan. 4, 2018) <http://www.investinblockchain.com/estonia-blockchain-model/> [<https://perma.cc/P3ZQ-3LLQ>].

¹⁴⁸ See *E-Identity*, E-ESTONIA (Mar. 20, 2018), <https://e-estonia.com/solutions/e-identity/id-card/> [<https://perma.cc/37RL-CWN4>].

¹⁴⁹ See *Frequently Asked Questions: Estonian Blockchain Technology*, E-ESTONIA, <https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf> [<https://perma.cc/4D2X-XDA4>].

Table 3: A 'Closed' or 'Permissioned' Blockchain Model with a TTP

No.	Group	Function	Permission
i.	Users	Propose new transactions	Closed: the TTP vets users before they can join, for instance to register land on the registry. ¹⁵⁰
ii.	Nodes	Store copies of the DL	Closed: the TTP acts as a single node, holding the master copy.
iii.	Miners	Propose new blocks	Closed: the TTP is the only party who updates the ledger.

3.2.2. A Trusted Nodes Model

[58] Commercial entities such as banks are also exploring ways to use blockchain to settle payments amongst themselves.¹⁵¹ In such cases, multiple parties could set up a system with a defined number of *trusted nodes* who each store copies of the blockchain.¹⁵² Since the number of trusted nodes is known, they could follow a less costly traditional, one-block-at-a-time consensus protocol, where nodes agree on each block to be added to the chain before continuing to the next block.¹⁵³

[59] Such closed platforms restrict control over the blockchain by limiting permission to store the ledger and add new blocks to a small number of trusted parties.¹⁵⁴ The platform can limit permission in respect

¹⁵⁰ For example, the land registry may require users to prove their identity, for instance through a government-issued ID, before giving them access to the system. In practice, in some jurisdictions, users may need to interact with a land registry through a lawyer or notary.

¹⁵¹ See *The R3 Story*, R3., <http://www.r3.com/about/> [<https://perma.cc/ZDK5-KMUJ>].

¹⁵² See Buterin, *Public and Private Blockchain*, *supra* note 138.

¹⁵³ See Bacon et al., *supra* note 12.

¹⁵⁴ See Buterin, *Public and Private Blockchain*, *supra* note 138.

of users, nodes, and miners, depending on the level of trust and desired functionality.¹⁵⁵ The table below shows a possible configuration.

Table 4: A ‘Closed,’ ‘Permissioned’ Blockchain Model with Trusted Nodes

No.	Group	Function	Permission
i.	Users	Propose new transactions	Closed: only authorised parties can join and participate.
ii.	Nodes	Store copies of the DL	Closed: only trusted nodes store copies of the ledger.
iii.	Miners	Propose new blocks	Closed: trusted nodes act as miners according to a consensus protocol.

[60] The result is a closed, permissioned platform with a *shared*—as opposed to distributed—ledger that should have lower running costs than distributed platforms, since there are fewer nodes. Moreover, the nodes may be able to process transactions more quickly, since transactions can be verified and blocks mined by a small number of trusted nodes, each with high processing power, as opposed to by thousands of distributed nodes.¹⁵⁶ As a result, they may provide a more scalable platform. However, the TTP or trusted nodes will need to invest in traditional security, to protect against hackers gaining access to the ledger or DoS attacks from taking down nodes.

3.3 Governance and Control

[61] A final aspect of trust relates to control over platform design: who has the power to determine how the platform operates? This raises issues of blockchain governance: who can change the platform and under what circumstances should past entries in the ledger be changed. In this section,

¹⁵⁵ *See id.*

¹⁵⁶ *See id.*

we first consider protocol changes, before turning to the reversibility of past transactions, and the role of service providers.

3.3.1. Developers and Protocol Changes

[62] From a technical perspective, governance involves the groups discussed above—users, miners and nodes—as well as a fourth group, the *developers*, who produce the software that nodes and miners run to support the blockchain.¹⁵⁷ In practice, blockchain governance will differ per platform. In the current cryptocurrency context, these four groups form a community around a shared interest in maintaining, and increasing, the value of the coin. Each group can use informal governance mechanisms to express its preferences. Examples include discussions of technical improvement proposals,¹⁵⁸ user-wide votes on protocol changes,¹⁵⁹ miner-implemented *soft forks*,¹⁶⁰ and ultimately, hard forks that lead to competing, alternative cryptocurrencies.¹⁶¹

¹⁵⁷ See NISTIR OVERVIEW, *supra* note 6, at 44.

¹⁵⁸ See, e.g., *Bitcoin Improvement Proposals*, GITHUB, <https://github.com/bitcoin/bips> [<https://perma.cc/2P39-THWT>] (providing an example of a governance mechanism used to express a preference); see also *Ethereum Improvement Proposals*, GITHUB, <https://github.com/ethereum/EIPs/issues/> [<https://perma.cc/S629-ZP7D>] (citing as an example of a governance mechanism).

¹⁵⁹ See, e.g., *CarbonVote*, CARBON VOTE, <http://carbonvote.com/> [<https://perma.cc/JYM3-NFH3>] (describing how user-wide voting works).

¹⁶⁰ See De Filippi & Loveluck, *supra* note 129, at 26.

¹⁶¹ See NISTIR OVERVIEW, *supra* note 6, at 33–34.

[63] For example, the Bitcoin source code is developed in an open-source manner using GitHub.¹⁶² Anybody can view the code and propose improvements.¹⁶³ However, only a small group, known as the *core developers* are able to make changes to the version of the software known as *Bitcoin Core*.¹⁶⁴ Thus, the Bitcoin platform is not fully open/permissionless at this code development level. Ethereum code is similarly developed through an open-source process, with the Ethereum Foundation having ultimate responsibility for code changes.¹⁶⁵ Ethereum's founder, Vitalik Buterin is a member of the foundation and actively participates in governance discussions.¹⁶⁶

Table 5. The Bitcoin Application of Blockchain Technology

No.	Group	Function	Permission
i.	Users	Propose new transactions	Open: Anyone can join the network and send and receive Bitcoin.
ii.	Nodes	Store copies of the DL	Open: Anyone can download the software and run a Bitcoin node.

¹⁶² See *Bitcoin Development*, BITCOINCORE, <https://bitcoin.org/en/development> [<https://perma.cc/2VKT-8QZD>]. Github is a web-based service that provides cloud-hosted distributed revision control and source code management for user-uploaded software projects. Anyone can register an account, create a software repository, and/or begin suggesting edits to other public repositories.

¹⁶³ See *How to Contribute Code to Bitcoin Core*, BITCOINCORE, <https://bitcoincore.org/en/faq/contributing-code/> [<https://perma.cc/C8Z7-349G>].

¹⁶⁴ See Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*, 17 NEVADA L.J. 139, 150 (2016).

¹⁶⁵ See Nick Tomaino, *The Governance of Blockchains*, THE CONTROL, (Feb. 28, 2017) <https://thecontrol.co/the-governance-of-blockchains-5ba17a4f5da6> [<https://perma.cc/J6MG-V4NY>].

¹⁶⁶ See *About the Ethereum Foundation*, ETHEREUM, <https://www.ethereum.org/foundation> [<https://perma.cc/DR79-HWKS>].

iii.	Miners	Propose new blocks	Open: Anyone can (attempt to) mine new blocks and broadcast them to the P2P network
iv.	Developers	Change the Bitcoin 'core' software	Closed: only a small group of core developers can change the 'core' code.

[64] Changes to the code encompass technical issues, like bug fixes, but also platform design decisions that have direct operational impact, such as the size of the blocks that determine the system's throughput. As a result, the platform requires users to place some level of trust in the developers.¹⁶⁷

[65] Nonetheless, the developers' power is limited by the possibility of *hard forks*.¹⁶⁸ Anyone can take the code from GitHub and *fork* it, meaning they can write a new version—typically an extension—of the software and make it available for others to download.¹⁶⁹ There are several versions of the Bitcoin software available that differ in terms of properties or functionality.¹⁷⁰

[66] This means that anyone can propose new technical features or platform designs, by writing new software with a different block size or consensus protocol. The deliberate creation of a new version of software that is incompatible with the existing software, for instance, because it has

¹⁶⁷ See Christopher, *supra* note 164, at 150; see also De Filippi & Loveluck, *supra* note 129, at 5 (discussing the extent to which trust plays into blockchain).

¹⁶⁸ See NISTIR OVERVIEW, *supra* note 6, at 33–34.

¹⁶⁹ See *id.*

¹⁷⁰ See, e.g., Fair Distribution, BITCOIN GOLD, <https://bitcoingold.org/> [<https://perma.cc/6VYY-DFV3>].

a different consensus protocol, is called a *hard fork*.¹⁷¹ In the case of a hard fork, miners and nodes must decide which version of the software they want to run.¹⁷² Different miners and nodes may choose to run different versions of the software. If they do, this creates two separate blockchains that track two different cryptocurrencies.¹⁷³ Both start from the last block before the fork but will add different blocks going forward. As a result, they will track two different cryptocurrencies.¹⁷⁴

[67] In practice, software is forked to provide some different functionality or capability.¹⁷⁵ To have impact, the resulting software must be adopted.¹⁷⁶ This means that each fork will need to attract miners, nodes, and users to their version of the software. The value of each currency resulting from a fork, is determined by supply and demand on currency exchanges.¹⁷⁷ This, in turn, depends on each currency's ability to attract miners, intermediaries, and ultimately, users.¹⁷⁸ The result is a system of

¹⁷¹ See NISTIR OVERVIEW, *supra* note 6, at 33–34.

¹⁷² See *id.*

¹⁷³ See *id.*

¹⁷⁴ See De Filippi & Loveluck, *supra* note 129, at 7 (providing for examples of such forks in relation to Bitcoin's block size). See generally *What is Segwit*, SEGWIT, <https://www.coindesk.com/information/what-is-segwit/> [<https://perma.cc/594Y-RQ5N>] (last updated Feb. 22, 2018).

¹⁷⁵ See NISTIR OVERVIEW, *supra* note 6, at 33–34.

¹⁷⁶ See *id.*

¹⁷⁷ See *id.*

¹⁷⁸ See Kyle Torpey, *You Really Should Run a Bitcoin Full Node: Here's Why*, BITCOIN MAG. (Mar. 9, 2017, 1:37 PM), <https://bitcoinmagazine.com/articles/you-really-should-run-full-bitcoin-node-heres-why/> [<https://perma.cc/8JPC-XGWL>]; Aaron van Wirdum, *On Consensus, or Why Bitcoin's Block-Size Presents a Political Trade-off*, BITCOIN MAG. (Jan. 15, 2016, 2:51 PM), <https://bitcoinmagazine.com/articles/on-consensus-or-why-bitcoin-s-block-size-presents-a-political-trade-off-1452887468/> [<https://perma.cc/2LNU-WMR4>].

checks and balances that should generally favour incremental protocol change.

[68] In more closed/permissioned and centralised instantiations of a DL, the code and its updates might be defined by agreements between the participants involved, including contractual agreements. Governance issues should be more straightforward where fewer parties are involved.

3.3.2 Reversibility of Past Transactions

[69] A second issue of blockchain governance relates to the reversibility of past transactions recorded on the blockchain. As discussed above, the blockchain aims to create a persistent, tamper-evident record of relevant transactions.¹⁷⁹ However, the ledger is not technically *immutable*.¹⁸⁰ The nodes of any given platform could undertake a coordinated effort to *correct* their local versions of the ledger and undo specific past transactions they considered inappropriate.¹⁸¹ The nodes would effectively *fork* to a new version of the blockchain without the offending transactions. Although this goes against the general aim of creating a persistent record, the nodes may agree that it is appropriate in exceptional circumstances.

[70] How easy this is to achieve differs according to the blockchain platform's design. On an open, distributed platform, establishing a hard fork is costly, both in terms of arranging cooperation between nodes and re-hashing previous blocks where required.¹⁸² A party seeking to reverse a past transaction would need to propose a network-wide hard fork.¹⁸³ There

¹⁷⁹ See discussion *supra* Section 2.1.

¹⁸⁰ See NISTIR OVERVIEW, *supra* note 6, at 33–34.

¹⁸¹ See *id.*

¹⁸² See Jeremy M. Sklaroff, *Smart Contracts and the Cost of Inflexibility*, 166 U. PA. L. REV., 263, 277 (2017).

¹⁸³ See NISTIR OVERVIEW, *supra* note 6, at 33–34.

is no guarantee that nodes will agree to fork. The difficulties are illustrated by the example of the Ethereum DAO, set out below in Section 6.6.¹⁸⁴

[71] Conversely, with a centralised platform, it should be easier to arrange a corrective fork. The TTP or small group of trusted nodes can agree to correct the ledger, which would also be less costly if the consensus protocol does not require PoW. Thus, a party seeking to reverse a past transaction would only need to submit a request to, and obtain approval of, the TTP or group of trusted nodes. As a result, centralised platforms can support reversibility better.

[72] A potentially simpler way to reverse the effects of a past transaction is for the parties to enter a *correcting transaction*, to be recorded in a subsequent block.¹⁸⁵ This second transaction would negate the effect of the initial transaction. However, this requires either both parties' cooperation, or at least access to the counter-party's private key if enforced externally by a third-party. As a result, this is not an option where one of the parties contests the reversal. Companies are also exploring the possibility of *editable* blockchains, changing the way hash pointers link blocks so that a small number of authorised parties can change past blocks.¹⁸⁶

3.3.3 Service Provider Considerations

[73] A final trust issue relates to the roles of service providers involved in the blockchain platform. As noted above, many users rely on intermediaries, such as online—or *hot*—wallets, as an interface to a

¹⁸⁴ See discussion *infra* Section 6.6.

¹⁸⁵ See Jeff John Roberts, *Why Accenture's Plan to 'Edit' the Blockchain Is a Big Deal*, FORTUNE (Sept. 20, 2016), <http://fortune.com/2016/09/20/accenture-blockchain/> [<https://perma.cc/V7GX-7VBY>].

¹⁸⁶ See *Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World*, ACCENTURE (2016), <https://newsroom.accenture.com/content/1101/files/Cross-FSBC.pdf> [<https://perma.cc/77E4-ZXGX>].

blockchain system.¹⁸⁷ This requires users to place some degree of trust in such service providers, since the provider determines the nature of the service and manages its operation.¹⁸⁸

[74] However, service providers may also be directly involved in the operation of a blockchain platform.¹⁸⁹ In such cases, sometimes termed *Blockchain-as-a-Service* (BaaS), a third party provides aspects of the platform's infrastructure.¹⁹⁰ This can range from a completely managed DL, to the hosting of particular nodes, as well as supporting infrastructure such as identity key management services.¹⁹¹ While BaaS is an emerging area, the major cloud providers are active in this space.¹⁹²

[75] BaaS raises additional trust and governance considerations, given the service provider's control over the technical infrastructure.¹⁹³ Ultimately, any concerns will depend on the precise nature of the service offered, and the degree of power the service provider has over the entire system. A provider managing a single node as part of a large, federated

¹⁸⁷ See Kevin D. Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, BERKELEY TECH. L.J. (forthcoming 2018) (manuscript at 27).

¹⁸⁸ See *id.*

¹⁸⁹ See Lucas Mearian, *Amazon Joins List of Blockchain-as-a-Service Providers*, COMPUTERWORLD FROM IDG (Jun. 1, 2018, 12:41 PM), <https://www.computerworld.com/article/3278088/blockchain/amazon-joins-list-of-blockchain-as-a-service-providers.html> [<https://perma.cc/AK22-9LZD>].

¹⁹⁰ See Jatinder Singh & Johan David Michels, *Blockchain as a Service (BaaS): Providers and Trust*, 2018 IEEE EUROPEAN SYMP. ON SECURITY & PRIVACY WORKSHOPS (EUROS&PW) (2018).

¹⁹¹ See *id.* at 12.

¹⁹² See Mearian, *supra* note 189.

¹⁹³ See Singh & Michels, *supra* note 190 (arguing that service providers detract from one of blockchain's most attractive attributes, a decentralised ledger).

network of nodes raises different considerations to a service provider that hosts all the nodes of a network. There are strong incentives for service providers to ensure the integrity of their platforms, as their reputation is crucial to the longevity of their business. Providers may also be able to use advances in technical mechanisms, such as trusted execution environments *secure enclaves* that aim to provide a technical guarantee that specific code was executed.¹⁹⁴

4. Visibility and Identity

[76] This section considers two further questions of blockchain platform design: (i) who can see the record of transactions stored on the blockchain and (ii) to what extent can the blockchain's users be identified.

4.1 Visibility of the Record: Public and Private Platforms

[77] As set out above, early cryptocurrencies are permissionless at the level of nodes and miners, meaning anyone can download the entire blockchain archive.¹⁹⁵ Further, all new transactions are broadcast to all nodes for the purpose of mining new blocks.¹⁹⁶ As a result, all blockchain transactions are publicly visible.¹⁹⁷ For instance, the latest Bitcoin transaction records are available to view online.¹⁹⁸ This record includes the sending Bitcoin address, the receiving Bitcoin address, the amount of Bitcoin, and a timestamp.¹⁹⁹ A Bitcoin address is a 26–35 digit

¹⁹⁴ See Singh & Michels, *supra* note 190, at 14.

¹⁹⁵ See discussion *supra* Section 3.

¹⁹⁶ See discussion *supra* Section 3.1.2.

¹⁹⁷ See Nakamoto, *supra* note 34, at 6.

¹⁹⁸ See *Latest Blocks*, BLOCK EXPLORER <https://blockexplorer.com/> [<https://perma.cc/XH3Q-H2AK>] (listing the latest blockchain blocks and transactions in real time).

¹⁹⁹ See *id.*

combination of letters and numbers which is generated based on a hash of a user's public key.²⁰⁰ Thus, the public can see that a particular address is sending an amount of Bitcoin to another address, but without information linking the addresses to any real-world identities.²⁰¹

[78] This public visibility of all transaction data may prove a barrier to the adoption of open, distributed platforms.²⁰² For certain use cases, parties may not be willing to share data about their transactions publicly, particularly where access to transaction data may provide a commercial advantage. For instance, if a blockchain were used for trading shares, competitors may be able to discern each other's trading patterns.²⁰³

[79] Conversely, more centralised systems can limit visibility of the blockchain to certain parties, resulting in a *private* blockchain.²⁰⁴ If a permissioned system is stored by a TTP, it can withhold access to the blockchain archive and grant permission to view blocks or entries only in specific cases.²⁰⁵ However, such a system asks for a higher degree of trust from users, since only the TTP will know whether the blockchain has been

²⁰⁰ See *Blockchain Address 101: What are Addresses on Blockchains?*, BLOCKGEEKS, <https://blockgeeks.com/guides/blockchain-address-101/> [<https://perma.cc/HL4Z-QTYA>].

²⁰¹ See NISTIR OVERVIEW, *supra* note 6, at 46.

²⁰² See *Technology Overview*, ZCASH, <https://z.cash/technology/index.html> [<https://perma.cc/D7TQ-74CX>] (stating that there are platforms that aim to use distributed blockchains without a publicly visible record. For example, Zcash features a blockchain that only stores encrypted data and uses a technique called 'zero knowledge proofs' for validation, without revealing the data).

²⁰³ See *Report: The Distributed Ledger Technology Applied to Secured Markets*, EUR. SEC. MKT. AUTHORITY, 11 (Feb. 7, 2017), https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf [<https://perma.cc/24K7-QMSK>].

²⁰⁴ See Buterin, *Public and Private Blockchain*, *supra* note 138.

²⁰⁵ See *id.*

tampered with.²⁰⁶ Similarly, in permissioned systems using trusted nodes, each trusted node stores and is able to view the entire blockchain.²⁰⁷ Since the blockchain is stored across multiple nodes, this type of system can limit visibility, while being more tamper-evident than systems with a single TTP.²⁰⁸

4.2 Identity of Participants

[80] In the physical world, we use birth certificates, passports, and other Government-issued official documents to prove our identity.²⁰⁹ On online networks, we often start from real-world documents, presenting them as credentials to institutions, for example when enrolling as a student at a university or registering with Airbnb. This is the basis for authentication, proving that you are who you say you are and allowing an electronic identity to be associated with a validated person and their real-world identity. Part of the establishment of an electronic identity is to associate electronic credentials such as a secret password or biometrics with the validated person.

[81] As noted above in Section 0, blockchains use PKI to authenticate users' identities.²¹⁰ Unlike Government-issued IDs, revealing a public key need not in general reveal the real-world identity of the associated party.²¹¹ As a result, even though each transaction record is public, Bitcoin and

²⁰⁶ *See id.*

²⁰⁷ *See id.*

²⁰⁸ *See id.*

²⁰⁹ *See, e.g., Acceptable Documents*, U.S. CITIZENSHIP & IMMIGR. SERV., <https://www.uscis.gov/i-9-central/acceptable-documents> [<https://perma.cc/8HEB-ERN5>] (listing various documents that can be used to prove your identity).

²¹⁰ *See* discussion *supra* Section 2.2.

²¹¹ *See* Nakamoto, *supra* note 34, at 6.

Ethereum users enjoy a level of anonymity by using their addresses as pseudonyms.²¹²

[82] To bolster their privacy, users could generate a new public key and address for each new transaction.²¹³ The public could still see that the Bitcoins had moved to a new address, but they would not know who controlled the new address. There are also other online services to help users mask their transactions, known as bitcoin *mixing* or *laundry*.²¹⁴

[83] In most cases, outside observers will not be able to determine the real-world identity of the parties to a transaction. Nonetheless, the two can be linked through a user's voluntary disclosure.²¹⁵ For instance, if a user pays an online merchant in Bitcoin, that merchant will likely ask for the customer's name, email address, and possibly real-world address.²¹⁶ Further, it may be possible to use other methods to de-anonymise users, such as by linking public keys to the IP addresses where the transactions are generated.²¹⁷ For example, a 2018 study claimed to identify 95 million Bitcoin addresses as belonging to 14 million identified individuals.²¹⁸

²¹² *See id.*

²¹³ *See* Jaume Barcelo, *User Privacy in the Public Bitcoin Blockchain*, 6 J. LATEX CLASS FILES 1, 1–2 (2017).

²¹⁴ *See, e.g.*, Thibault de Balthasar & Julio Hernandez-Castro, *An Analysis of Bitcoin Laundry Services*, 10674 LECTURE NOTES IN COMPUTER SCI., 297, 297–98 (2017) (describing various mixer and laundry services).

²¹⁵ *See* Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, in SEC. & PRIV. IN SOC. NETWORKS 197, 212 (Yaniv Altshuler et al. eds. 2013).

²¹⁶ *See id.* at 210.

²¹⁷ *See* Alex Biryukov et al., *Deanonymisation of Clients in Bitcoin P2P Network*, 2014 PROC. ACM SIGSAC CONF. ON COMPUTER AND COMM. SEC. 16, 21.

²¹⁸ *See* Bitfury *De-Anonymises Millions of Bitcoin Transactions and Addresses*, TRUSTNODES (Jan. 9, 2018, 3:39PM), <http://www.trustnodes.com/2018/01/09/bitfury-de-anonymises-millions-bitcoin-transactions-addresses> [<https://perma.cc/QFR6-E5KK>].

Anyone who knows the real-world identity associated with a Bitcoin address, can review the entire transaction history associated with that address.²¹⁹

[84] Future blockchain platforms may instead require the real-world identity of participants to be established, rather than hidden. This will likely depend on the functionality they seek to offer and on regulatory requirements. For instance, a number of organisations are promoting the use of blockchain to allow individuals to manage their identity.²²⁰ In such cases, an individual would probably need to verify their identity using traditional methods to a TTP, who would then vouch for that individual's identity.²²¹

5. Smart Contracts

[85] Section 3.1 above described the core components of blockchain software that enable users to submit transactions securely to a tamper-evident data structure of linked blocks.²²² Some blockchain applications might feature single, standalone transactions, which are relatively simple to incorporate into a ledger, such as a Bitcoin transfer from one party to another. Other applications might require more complicated interactions, such as a series of related, sequential or conditional transactions.²²³ For

²¹⁹ See Barcelo, *supra* note 213, at 2.

²²⁰ See Reed et al., *supra* note 16, at 14–15 (discussing the notion of self-sovereign identity).

²²¹ See, e.g., *Public Key Certificates*, MICROSOFT (May 30, 2018), <https://docs.microsoft.com/en-us/windows/desktop/seccertenroll/about-x-509-public-key-certificates> [<https://perma.cc/E5ZV-2VFQ>] (defining “public key certificates”); *CA Certificate*, MICROSOFT SEC. GLOSSARY (May 30, 2018), <https://docs.microsoft.com/en-us/windows/desktop/SecGloss/c-gly#-security-certification-authority-gly> [<https://perma.cc/VRA2-E724>] (defining “CA certificate”). See generally Bacon et al., *supra* note 12 (providing details on Certification Authorities).

²²² See *supra* notes 62–64 and accompanying text.

²²³ See NISTIR OVERVIEW, *supra* note 6, at 35.

example, an international supply chain would require a great deal of documentation to be verified as goods travel from source to destination. Their progress could be documented on a blockchain, to record that the goods have arrived at and departed from various intermediate locations.

[86] Smart contracts can be used to automate such a series of transactions.²²⁴ Introduced by Szabo in 1994, a smart contract is “a computerised transaction protocol that executes the terms of a contract.”²²⁵ The term *smart contract* may confuse lawyers, since it does not refer to a legal contract, see Section 6.1 below. Instead, the term essentially refers to a computer program that automatically brings about some specified action, such as carrying out transfers of, or executing other actions relating to, digital assets according to a set of pre-specified rules.²²⁶ As a result, smart contracts can be used to automate agreements between parties according to the set of instructions written into their code.²²⁷ In many ways, smart contracts resemble the stored procedures and/or triggers, *event-condition-action* rules, which are common in relational databases.²²⁸

²²⁴ See Dawei Ding, *Smart Contracts to Enable Automated Transactions*, BCF BUS. L. (Mar. 23, 2018), <http://www.bcf.ca/en/current-affairs/907/smart-contracts-to-enable-automated-transactions> [<https://perma.cc/LDV5-M4YF>].

²²⁵ Nick Szabo, *Smart Contracts*, PHONETIC SCI., AMSTERDAM (1994) [hereinafter Szabo, *Smart Contracts*], <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> [<https://perma.cc/KP3Y-AURX>]; see also Nick Szabo, *The Idea of Smart Contracts*, PHONETIC SCI., AMSTERDAM (1997) [hereinafter Szabo, *Idea of Smart Contracts*], <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html> [<https://perma.cc/4858-8NNY>] (discussing smart contracts and the kinds of contractual clauses involved).

²²⁶ See Szabo, *Smart Contracts*, *supra* note 225; Buterin, *ETHEREUM WHITE PAPER* *supra* note 109, at 1.

²²⁷ See NISTIR OVERVIEW, *supra* note 6, at 35.

²²⁸ See Konstantinos Christidis & Michael Devetsikiotis, *Blockchains and Smart Contracts for the Internet of Things*, 4 IEEE ACCESS, 2296–97 (2016).

[87] Smart contracts thus aim to capture in software the semantics of potentially complex interactions.²²⁹ The workflows that represent a complex interaction may be represented as a number of transactions, triggered as appropriate as the interaction progresses. The challenges involved in correctly capturing these semantics as smart contracts include validation and verification.²³⁰

[88] A further platform design consideration is therefore the extent to which the platform will support user-made smart contracts, alongside predefined smart contracts that form part of the platform's basic functionality. The more a blockchain platform supports smart contracts, the more scope users have to use the platform for different purposes. Developers who want to create a simple blockchain for a predetermined purpose may opt to offer limited support for smart contracts, or only support smart contracts made of predefined components. In Bitcoin, the functionality relating to transactions is brought about through a series of scripts or programs.²³¹ These scripts can be used to control Bitcoins thereby supporting basic smart contracts with limited functionality.²³²

[89] Conversely, developers can also allow their platform to support many types of smart contract.²³³ A key feature of Ethereum is that it supports *Turing-complete* smart contracts.²³⁴ Turing-completeness means that the language is as fully-featured as a general programming language

²²⁹ See, e.g., NISTIR OVERVIEW, *supra* note 6, at 35.

²³⁰ See Daniele Maggazeni et al., *Validation of Smart Contracts: A Research Agenda*, IEEE COMPUT. SOC'Y, at 50 (Sept. 2017).

²³¹ See Aviv Zohar, *Bitcoin: Under the Hood*, 58 COMM. ACM, 9, 104, 110–11 (2015); see also NISTIR OVERVIEW, *supra* note 6, at 40.

²³² See Buterin, ETHEREUM WHITE PAPER, *supra* note 109, at 11–12.

²³³ See *id.* at 12.

²³⁴ See *id.* at 1, 12–13.

and is not restricted in what it can compute.²³⁵ As a result, Ethereum can be used as a platform to run a wide array of applications expressed in smart contracts,²³⁶ as opposed to Bitcoin's *Script* which is deliberately limited in scope.²³⁷ Given this, some authors differentiate between Ethereum as a platform and Bitcoin as a digital currency.²³⁸

[90] In terms of operation, as part of the block mining process, a transaction, i.e. a ledger entry, being processed might trigger a smart contract. This results in the smart contract's code being executed, where the triggering and any resulting transactions, i.e. contract outputs, are encoded in the block along with any other transactions forming the block.²³⁹ As part of the block validation process, all nodes will also execute and verify the contract to ensure that the smart contract was properly executed.²⁴⁰ In other words, as per Buterin: "if a transaction is added into block B the code execution spawned by that transaction will be executed by all nodes, now and in the future, that [. . .] validate block B."²⁴¹ In this way, smart contracts enable consensus regarding

²³⁵ See *id.* at 28, 34.

²³⁶ See *id.* at 34.

²³⁷ See Andreas M. Antonopoulos, *Mastering Bitcoin: Chapter 5. Transactions*, O'REILLY, <https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch05.html> [<https://perma.cc/GH3T-UJRU>].

²³⁸ See Paolo Tasca et al., *Taxonomy of Blockchain Technologies. Principles of Identification and Classification*, ALLQUANTOR (May 31, 2017), <https://allquantor.at/blockchainbib/pdf/tasca2017ontology.pdf> [<https://perma.cc/4GNH-346K>].

²³⁹ See Buterin, ETHEREUM WHITE PAPER, *supra* note 109, at 7.

²⁴⁰ See *id.* at 10.

²⁴¹ *White Paper: A Next-Generation Smart Contract and Decentralized Application Platform*, GITHUB, <https://github.com/ethereum/wiki/wiki/White-Paper#a-next-generation-smart-contract-and-decentralized-application-platform> [<https://perma.cc/BL32-R5WY>].

computation,²⁴² given that generally all nodes in a network will verify a contract's execution.²⁴³ Since smart contract code is generally run on all nodes on the network, it is publicly visible to all participants, meaning the code can be inspected and re-used by other participants.²⁴⁴

III. BLOCKCHAIN AND THE LAW

6. Legal Analysis

[91] In Part One, above, we saw that blockchain technology can be applied in various ways to create platforms with different features, including with regard to:

- (i) Access: who can propose new transactions to be added to the ledger;
- (ii) Control:
 - a. Storage: who stores a copy of the ledger;
 - b. Mining and consensus: how to create new blocks and determine when blocks should be added to the existing ledger;
 - c. Governance: who controls the platform's underlying software;
- (iii) Visibility: who can view the ledger;
- (iv) Identity: whether users are identifiable; and,
- (v) Automation: whether the platform supports smart contracts.

[92] In this section we argue that these variables may be significant from a legal perspective. To illustrate this point, we look at various ways in which blockchain technology is being used to create structures that resemble existing legal concepts, including contracts, companies, and

²⁴² See Ahmed Kosba et al., *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*, IEEE SYMP. ON SEC. & PRIV. 839, at 839 (2016).

²⁴³ See Buterin, *ETHEREUM WHITE PAPER*, *supra* note 109, at 4, 6–7.

²⁴⁴ See *id.* at 1.

securities. Below, we consider how existing law will apply to these new blockchain-based structures. We will consider, in turn, issues arising under (i) contract law, (ii) data protection law, (iii) securities law, (iv) property law, (v) intellectual property and finally (vi) company law. For each area, we illustrate how the legal analysis is affected by the way in which blockchain technology is deployed in a specific use case.

6.1 Smart Contracts and Contract Law

6.1.1 Formation: Is a Smart Contract a Contract?

[93] The term *smart contract* is arguably misleading, since it refers to automatically executing computer code, see Section 5.²⁴⁵ This raises the question whether a smart contract qualifies as a legal contract.

[94] A legal contract is commonly defined as a legally enforceable agreement or promise.²⁴⁶ It is typically formed through voluntary offer and acceptance, as well as—in common law jurisdictions—consideration: the value offered by each party.²⁴⁷ Many types of contracts can be established in any form: orally, in writing, or through actions, such as assenting to terms in electronic media by clicking, also known as *clickwrap agreements*.²⁴⁸ However, the law in some countries may require that certain types of contracts be recorded in a specific form or be entered into

²⁴⁵ See discussion *supra* Section 5.

²⁴⁶ See, e.g., *Contract*, BLACK'S LAW DICTIONARY (2d ed. 2018), <https://thelawdictionary.org/contract/> [<https://perma.cc/FRQ8-H94Y>] (providing a definition of contract).

²⁴⁷ See RESTATEMENT (SECOND) OF CONTRACTS § 1 cmt. b, d (AM. LAW INST. 1981); see also RESTATEMENT (SECOND) OF CONTRACTS § 17 (AM. LAW INST. 1981); RESTATEMENT (SECOND) OF CONTRACTS § 71 (AM. LAW INST. 1981).

²⁴⁸ See, e.g., W. Kuan Hon et al., *Negotiated Contracts for Cloud Services*, in CLOUD COMPUTING L. (Christopher Millard ed., 2013), 76-77; see RESTATEMENT (SECOND) OF CONTRACTS § 4 (AM. LAW INST. 1981).

in a particular manner, for instance requiring real estate transactions to be recorded in writing and witnessed by a notary.²⁴⁹

[95] One could argue that a smart contract is not a legally enforceable *promise*, but an automated mechanical process.²⁵⁰ While this may be true at the level of the computer-readable code, it is unlikely to reflect smart contract use in practice. In reality, the creator of a smart contract will ordinarily need to explain his offer to human counter-parties in human-intelligible language. This explanation can form the basis of the agreement between the parties and thereby determine the terms of the contract.

[96] For example, assume party A sets up a crypto-asset exchange contract on Ethereum. The smart contract's instructions are that if a counter-party pays 1 ETH into a specified address, it will in return provide them with a 'CryptoKitty,' a unique cartoon cat, stored on the blockchain.²⁵¹ In order to attract human counter-parties to this offer, A will have to explain it to them in a language they can understand, for instance through a website like <https://www.cryptokitties.co/> or other user interface. In doing so, A will communicate the details of her offer. By engaging with the smart contract—in this instance, paying 1 ETH to a specific address—B expresses acceptance, assenting to the terms of A's offer as explained in the user interface.²⁵² Even though the underlying

²⁴⁹ See RESTATEMENT (SECOND) OF CONTRACTS § 110 (AM. LAW INST. 1981).

²⁵⁰ See Kevin Werbach & Nicolas Cornell, *Contracts Ex. Machina*, DUKE L.J. 313, 339–40 (2017).

²⁵¹ See Fitz Tepper, *People Have Spent Over \$1M Buying Virtual Cats on the Ethereum Blockchain*, TECH CRUNCH (Dec. 3, 2017), <https://techcrunch.com/2017/12/03/people-have-spent-over-1m-buying-virtual-cats-on-the-ethereum-blockchain/> [<https://perma.cc/N298-TM24>].

²⁵² See Werbach & Cornell, *supra* note 250, at 340–41.

smart contract code may technically be visible,²⁵³ many users will likely *de facto* rely on A's other communications.

[97] Parties offering smart contracts may seek, via disclaimers or other provisions in their Terms of Service, to limit their contractual obligations solely to the computer-readable code.²⁵⁴ For instance, in 2016, the website of *The DAO*—a collection of smart contracts set up on the Ethereum blockchain—stated explicitly in its terms of service that the smart contract was the valid legal agreement.²⁵⁵ Any human-readable documents or explanations on the accompanying website were “merely offered for educational purposes” and could not override the terms of the code.²⁵⁶

[98] Whether such disclaimers are legally binding may be tested in court. On the one hand, standard contracts commonly include provisions that exclude all representations outside of the contract terms and provide a hierarchy between various legal documents.²⁵⁷ Moreover, given that smart contract code is typically visible to all nodes on the blockchain, their function should be legible to a skilled programmer/developer. On the other hand, simply publishing machine-readable code may not provide sufficient

²⁵³ See, e.g., *Contract 0x06012c8cf97BEaD5deAe237070F9587f8E7A266d*, ETHERSCAN, <https://etherscan.io/address/0x06012c8cf97bead5deae237070f9587f8e7a266d#code> [<https://perma.cc/6WFM-YVYT>].

²⁵⁴ See Werbach & Cornell, *supra* note 250, at 350–51.

²⁵⁵ See *Explanation of Terms and Disclaimer*, THE DAO (Apr. 27, 2016), <https://web.archive.org/web/20160704190119/https://daohub.org/explainer.html> [<https://perma.cc/EWT9-PUTY>].

²⁵⁶ *Id.*

²⁵⁷ See Gregory Klass, *Interpretation and Construction in Contract Law*, 1, 26 (Jan. 2018) (draft manuscript) (citing *W. W. W. Assoc. v. Giancontieri*, 566 N.E.2d 639, 642 (N.Y. 1990)) <http://scholarship.law.georgetown.edu/facpub/1947> [<https://perma.cc/XUU2-7J9W>]; see also *Hierarchy of Documents Sample Clauses*, LAW INSIDER, <https://www.lawinsider.com/clause/hierarchy-of-documents> [<https://perma.cc/EJH4-UUGG>].

notice of contractual terms to non-expert counter-parties.²⁵⁸ Further, if there is an obligation that some term should be *fair and reasonable*—typically an exclusion or limitation of liability—that has to be assessed individually in relation to the parties.²⁵⁹ A term might be generally fair and reasonable, but not so in the particular circumstances.²⁶⁰

[99] Given the above, the code may be more likely to be binding in B2B-cases, than in B2C or C2C cases. Further, the code could be binding if the counter-party also uses a smart contract to express their assent, i.e. a machine-to-machine smart contract. The two smart contracts will find agreement only if there is a set of computer-readable terms that are acceptable to both parties. In such cases, there is a strong argument for limiting the contract's obligations to those expressed in the code.

[100] However, even machine-to-machine smart contracts' terms may not be legally binding in all cases.²⁶¹ Many jurisdictions limit parties' contractual freedom by determining that certain contractual terms are not enforceable, for instance in order to address power asymmetries between the contracting parties—such as between producers/retailers and consumers; landlords and tenants; or employers and employees—or because the terms are otherwise unconscionable.²⁶² For example, a smart contract that does not give a consumer a right of withdrawal or refund may fall foul of consumer protection law.

²⁵⁸ See Pierluigi Cuccuru, *Beyond Bitcoin: An Early Overview on Smart Contracts*, INT'L J.L. INFO. TECH. 179, 188–89 (2017).

²⁵⁹ See *Cleaver v. Schyde* (2011) EWCA Civ 929, [2011] 2 P. & C.R. 21 (UK).

²⁶⁰ See *id.*

²⁶¹ See Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 325 (2017).

²⁶² See *id.* at 325, 328; see also Werbach & Cornell, *supra* note 250, at 347, 350.

6.1.2 Performance: Can Smart Contracts be Breached?

[101] Since smart contracts self-execute pre-determined code, it could be argued that they cannot be breached.²⁶³ The smart contract will always do exactly what it says in its code. However, as noted above, the legal contract between the parties is likely to include obligations beyond the code itself, based on other communications.²⁶⁴ If that is the case, not all of the obligations can be captured fully and correctly by the underlying smart contract. As a result, there may be a mismatch between what the parties have agreed and what the smart contract's code executes, resulting in non-performance.²⁶⁵ Smart contracts are by their nature limited to those contractual terms that can be specified in computer-readable code,²⁶⁶ and further limited by any constraints imposed by the blockchain system in which the contract operates. As a result, they are unable to capture the real-world complexity of all but the simplest transactions.²⁶⁷

[102] Contractual performance²⁶⁸ in transactions involving digital assets, such as the exchange of crypto-assets described above, is relatively straightforward to describe and measure. The ledger then provides a reliable record of the transactions and contracts executed.²⁶⁹ However, the complexity of transactions is magnified if performance involves off-chain,

²⁶³ See Raskin, *supra* note 261, at 322.

²⁶⁴ See Werbach & Cornell, *supra* note 250, at 331, 342.

²⁶⁵ See Eliza Mik, *Smart Contracts: Terminology, Technical Limitations and Real-World Complexity*, 9.2 L., INNOVATION, & TECH. 1, 11 (2017).

²⁶⁶ See Werbach & Cornell, *supra* note 250, at 343.

²⁶⁷ See Karen Levy, *Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law*, 3 ENGAGING SCI., TECH., & SOC'Y 1, 10 (2017); see also Mik, *supra* note 265, 22 (2017).

²⁶⁸ I.e. the performance of a legal contract, not performance in the computer science sense.

²⁶⁹ See Levy, *supra* note 268, at 2.

real world assets, such as giving access to a vehicle through a smart lock.²⁷⁰ In such cases, performance is harder to assess; the quality of the service may be below a reasonable standard, e.g. the vehicle may not start, or otherwise differ from reasonable expectations.²⁷¹

[103] Where performance is disputed, the parties may seek to address this through negotiation, arbitration, or litigation. Thus, while smart contracts might simplify execution, they will not prevent contractual disputes. Nonetheless, the blockchain's consensus mechanisms may give guarantees about the smart contracts that were executed and the surrounding circumstances.

6.1.3 Modification and Enforcement: Are Mistakes in Smart Contracts Reversible?

[104] The code of smart contracts is subject to human error and is therefore likely to contain bugs.²⁷² Mistakes in the code may prove costly.²⁷³ For instance, if an attacker exploits a poorly-written smart contract, any resulting transactions are written into the tamper-evident blockchain. The offering party can replace the smart contract for future transactions, but cannot edit the existing smart contract or easily reverse its effects.²⁷⁴ For example, in 2017, a user accidentally triggered a flaw in the code of a smart contract service called Parity.²⁷⁵ The service provided

²⁷⁰ See Mik, *supra* note 265, at 22.

²⁷¹ See Raskin, *supra* note 261, at 326.

²⁷² See Werbach & Cornell, *supra* note 250, at 365.

²⁷³ See Mik, *supra* note 265, at 11.

²⁷⁴ See *id.* at 7, 11.

²⁷⁵ See, e.g., Alex Hern, *\$300m in Cryptocurrency Accidentally Lost Forever Due to Bug*, THE GUARDIAN (Nov. 12, 2017, 6:29 PM), https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether?CMP=share_btn_tw [<https://perma.cc/7TA5-3YKF>].

multi-signature wallets for Ethereum.²⁷⁶ As a result, an estimated 1m ETH, worth U.S. \$300 million at the time, was permanently frozen in the wallets, with no way for users to access their funds.²⁷⁷

[105] Mistakes in legal contracts may be costly too. However, since a legal contract is not self-executing, a party can withhold performance and renegotiate terms.²⁷⁸ In the event of an on-going dispute, the parties can turn to litigation. A judge may then be able to correct obvious mistakes or incompleteness in contract language through interpretation, by assessing the intent of the parties.²⁷⁹ Thus, parties can seek to correct mistakes in legal contracts after signing.

[106] Resolving mistakes in smart contracts is more complicated. Since a smart contract is self-executing, its automated performance is written into the blockchain.²⁸⁰ As outlined in Section 3.3.2, reversing past blockchain transactions would require either a *correcting transaction*, or encouraging the other participants in a blockchain network to initiate a *hard-fork*.²⁸¹ As explained above, centralised platforms can support reversibility better than distributed platforms.²⁸² For example, the only way to release the *frozen* Parity funds is reportedly through an Ethereum hard fork.²⁸³ While the

²⁷⁶ See *id.*

²⁷⁷ See *id.*

²⁷⁸ See Sklaroff, *supra* note 182, at 277–78.

²⁷⁹ See Werbach & Cornell, *supra* note 250, 369, 374.

²⁸⁰ See Jenny Cieplak & Simon Leefatt, *Smart Contracts: A Smart Way to Automate Performance*, 1 GEO. L. TECH. REV. 414, 418 (2017).

²⁸¹ See NISTIR OVERVIEW, *supra* note 6, at 33–34.

²⁸² See discussion *supra* Section 3.3.2.

²⁸³ See Hern, *supra* note 275.

Parity team has proposed such a *hard fork*,²⁸⁴ as of March 2018, it appeared unlikely that the rest of the Ethereum participants would agree to one.²⁸⁵

[107] It may be possible to incorporate logic for unwinding a transfer into the smart contract at the outset. For instance, enforcement of the contract could, in theory, be structured to allow for arbitration by a third-party adjudicator with their own private key.²⁸⁶ This would however reintroduce a requirement of trust in a third party and add a further layer of complexity to the code. It is not clear at present who these adjudicators would be or what procedural and substantive rules they would apply in resolving disputes.²⁸⁷

[108] As explained in Section 3.3.2 above, centralised platforms can support reversibility better. As a result, with a centralised platform, it should be easier to arrange a corrective fork. The TTP or small group of trusted nodes can agree to correct the ledger.²⁸⁸

²⁸⁴ See *On Classes of Stuck Ether and Potential Solutions*, PARITY TECH (Dec. 11, 2017), <https://paritytech.io/blog/on-classes-of-stuck-ether-and-potential-solutions-2.html> [<https://perma.cc/XE36-4W76>].

²⁸⁵ See Rachel Rose O'Leary, *High Stakes: Ethereum's Fight Over Lost Funds Explained*, COINDESK (Feb. 25, 2018, 10:31 PM), <https://www.coindesk.com/high-stakes-ethereums-fight-lost-funds-explained/> [<https://perma.cc/9XNY-KVSU>].

²⁸⁶ See Vitalik Ruterin, *Multisig: The Future of Bitcoin*, BITCOIN MAG. (Mar. 12, 2014), <https://bitcoinmagazine.com/11108/multisig-future-bitcoin/> [<https://perma.cc/AXJ9-K5JF>]; see also Werbach & Cornell, *supra* note 250, at 375.

²⁸⁷ See Sklaroff, *supra* note 182, at 300–01.

²⁸⁸ See discussion *supra* Section 3.3.2.

6.1.4 Confidentiality and Trade Secrets

[109] As noted above in Section 5, the code of a smart contract is executed by all nodes on the network and is publicly visible.²⁸⁹ However, many contracts contain commercially sensitive information.²⁹⁰ Thus, smart contracts are inappropriate for contracts that contain information that would otherwise be subject to a non-disclosure agreement or confidentiality clause. In a worst-case scenario, revealing information through a smart contract could lead to inadvertent loss of trade secret protection or to a breach of confidentiality. This is less of an issue on centralised platforms, where the TTP or trusted nodes can control visibility of the blockchain.

6.2 Blockchain Data and the GDPR

[110] The application of EU data protection law to blockchain-based platforms raises difficult questions. In this section, we first consider data protection law's applicability, before reviewing who would qualify as controllers or processors and considering compliance and liability.

6.2.1 Will Data Protection Laws Apply?

[111] EU data protection laws apply to the processing of personal data that falls within the regime's territorial scope.²⁹¹ The General Data

²⁸⁹ See discussion *supra* Section 5.

²⁹⁰ See David Cerezo Sánchez, *Private and Verifiable Smart Contracts on Blockchains*, CALCTOPIA 2 (May 20, 2018), <https://eprint.iacr.org/2017/878.pdf> [<https://perma.cc/5CSA-ZDLJ>].

²⁹¹ See *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, (General Data Protection Regulation), OJ 2016 L 119/1, art. 3 [hereinafter GDPR].

Protection Regulation (GDPR)²⁹² entered into force in May 2018 and has a broad territorial reach. The GDPR applies to controllers and processors *established* in the EU.²⁹³ Existing case law suggests that the test for establishment will be applied expansively.²⁹⁴ The GDPR also applies to controllers and processors not established in the EU, where the processing relates to the offering of services to data subjects who are in the EU or monitoring of their behaviour that takes place within the EU.²⁹⁵

[112] As a result, the activities of many blockchain operators will fall within the regime's territorial scope. For example, since anybody can use an open/permissionless platform, operators of such platforms may be deemed to offer services to data subjects in the EU. For instance, it could be argued that the nodes and miners who collectively support the Bitcoin network offer a payment service to EU data subjects. In contrast, to avoid the GDPR's applicability, non-EU-established operators of closed/permissioned platforms could attempt to prevent data subjects located in the EU from using their platforms.

[113] *Processing* is broadly defined. It refers to any operation or set of operations performed on personal data.²⁹⁶ As a result, blockchain users,

²⁹² *See id.*

²⁹³ *See id.* at art. 3(1).

²⁹⁴ *See* Google Spain v. Agencia Española de Protección de Datos, C-131/12, § 54–59 (E.C.J. May 13, 2014) [hereinafter Google Spain v. González] (stating the concept of establishment was interpreted so as to provide a broad territorial scope in order to “prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented . . .”).

²⁹⁵ *See* GDPR, *supra* note 291, at art. 3(2) (constituting a change from the test in the Data Protection Directive, which focused on use of ‘equipment’ in the EU rather than offering services to or monitoring the behavior of data subjects in the EU. Both approaches, however, are potentially overly broad in scope); *see also* W. Kuan Hon, Julia Hörnle & Christopher Millard, *Which Law(s) Apply to Personal Data in Clouds?*, in CLOUD COMPUTING LAW (Christopher Millard ed., 2013).

²⁹⁶ *See* GDPR, *supra* note 291, art. 4(2).

nodes, and miners may engage in processing of personal data when sending, verifying, and storing transaction data.²⁹⁷

[114] The definition of *personal data* is also very expansive. It covers any information that relates to an identifiable person, i.e. a person who can be identified *directly or indirectly*.²⁹⁸ To determine whether a person can be indirectly identified, account should be taken of all the means likely reasonably to be used by the controller or by any other party to identify the person.²⁹⁹

[115] A blockchain database is likely to contain at least two types of data. First, it will store metadata related to transactions, namely the sender's and recipient's addresses and a timestamp.³⁰⁰ Second, it will store data on the object of a transaction.³⁰¹ For instance, in the case of Bitcoin, the object would be an amount of BTC.³⁰² We will now consider each of these in turn.

i. Metadata as Personal Data

[116] With respect to metadata, if the platform's users are natural persons, the sender's and recipient's addresses may well qualify as personal data. This is most obvious where these addresses directly reveal a person's identity. For specific applications, for example a land registry blockchain, titles to property may be transferred from one named

²⁹⁷ See Michèle Finck, *Blockchains and Data Protection in the European Union*, Research Paper No. 18-01 MAX PLANCK INST. FOR INNOVATION & COMPETITION 1, 9–10, (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322.

²⁹⁸ See GDPR, *supra* note 291, at art. 4(1).

²⁹⁹ See *id.* at Recital 26.

³⁰⁰ See NISTIR OVERVIEW, *supra* note 6, at 20.

³⁰¹ See *id.*

³⁰² See *id.* at 40.

individual to another. While a platform operator may opt to *pseudonymise* the data, by replacing a person's name with a pseudonym, the GDPR makes it clear that such pseudonymised data will still qualify as personal data.³⁰³

[117] Even Bitcoin's disposable public keys and addresses may qualify as personal data.³⁰⁴ The ECJ has determined that information can constitute personal data even where only a third party has the additional data necessary to identify the person.³⁰⁵ In such cases, whether information is personal data may depend on whether the possibility of combining the two sources is "a means likely reasonably to be used" to identify the data subject.³⁰⁶

[118] Although there is no central register matching addresses to individuals, a Bitcoin address might still be linked to a real-world identity by combining it with other data.³⁰⁷ Intermediaries, such as wallet services or exchanges, may register users' real-world identities, for instance to comply with regulatory requirements.³⁰⁸ Further, the counter-parties a user transacts with, such as merchants, may register users' real-world identities for their own commercial purposes.³⁰⁹ Combining intermediary records with the public blockchain would reveal the real-world identity behind a Bitcoin address.

³⁰³ See GDPR, *supra* note 291, at Recital 26.

³⁰⁴ See Finck, *supra* note 297, at 13–14.

³⁰⁵ See Breyer v. Germany, C-582/14, § 31, 39 (E.C.J. 2016).

³⁰⁶ See *id.* at § 45.

³⁰⁷ See Reid & Harrigan, *supra* note 215, at 211.

³⁰⁸ See Ana Alexandre, *US: Cryptocurrency Trading Platforms Must Be Registered with SEC*, COINTELEGRAPH (Mar. 7, 2018), <https://cointelegraph.com/news/us-cryptocurrency-trading-platforms-must-be-registered-with-sec> [<https://perma.cc/FF86-JVM3>].

³⁰⁹ See Reid & Harrigan, *supra* note 215, at 201.

[119] In addition, as noted in Section 4.2 above, it may be possible to determine Bitcoin user identities by other methods, such as linking public keys to IP addresses.³¹⁰ Finally, metadata may reveal a pattern of transactions with publicly known addresses (such as merchants) that could be used to single out an individual user, such as through a technique known as *transaction graph analysis*.³¹¹ For example, if a certain restaurant accepts Bitcoin as payment and its address is publicly known, then payments to that address would suggest that the sender visited that restaurant at a certain time.³¹² Given this, Bitcoin addresses and public keys might in certain circumstances qualify as personal data.

[120] Conversely, if a platform's users are all legal persons, such as businesses, the platform could be designed such that the metadata does not contain information related to natural persons. For example, a group of banks could set up a closed/permissioned platform to settle end-of-day inter-bank payments for their own accounts, i.e. reflecting the sum total of individual transactions at the inter-bank level. In this case, the addresses might refer only to the sending and receiving banks in question and need not relate to any identifiable person.

ii. Object of Transactions Data as Personal Data

[121] With respect to the object of transactions, in many use cases, this information will not relate to an identifiable person. For instance, in Bitcoin, the amount of BTC transferred does not necessarily relate to an identifiable person,³¹³ nor would payment data for an overall end-of-day settlement between banks.

³¹⁰ See Biryukov et al., *supra* note 217, at 15.

³¹¹ See Adam Ludwin, *How Anonymous Is Bitcoin?*, COIN CTR. (Jan. 20, 2015), <https://coincenter.org/entry/how-anonymous-is-bitcoin> [<https://perma.cc/4RTP-AMJY>].

³¹² See *id.*

³¹³ In some cases, the amount paid could be combined with information about the recipient address to specify the product or service paid for, which may help 'single out' the sender.

[122] Nonetheless, in other use cases, the object of the transaction could be linked to real-world identities. For example, a group of retail banks could set up a blockchain platform to share KYC (Know Your Customer) information on their customers with each other. In that case, the object of transactions would be information about natural persons and could be written into the blockchain.

[123] However, it may be possible to design a blockchain platform such that any personal data is not stored *on the chain*, but is stored in encrypted form in a separate, *off-chain* database.³¹⁴ The blockchain transaction data would then only contain the information needed to access the personal data in the separate database.³¹⁵ In this manner, it may be possible to confine personal data to the off-chain storage and avoid storing such data on the blockchain.

6.2.2 Who Will be Subject to Legal Obligations as Controller(s) and Processor(s)?

[124] Data controllers and processors are responsible for ensuring compliance with data protection law. The controller is the natural or legal person who determines the purposes and means of processing personal data.³¹⁶ The ECJ has held that *controller* should be interpreted broadly, so as to ensure the effective and complete protection of data subjects.³¹⁷ A processor is any natural or legal person who processes personal data on behalf of the controller.³¹⁸

³¹⁴ See Finck, *supra* note 297, at 11–12.

³¹⁵ See Guy Zyskind et al., *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, IEEE SECURITY PRIVACY WORKSHOPS (2015).

³¹⁶ See GDPR, *supra* note 291, at art. 4(7).

³¹⁷ See *Google Spain v. Agencia Española de Protección de Datos*, C-131/12, § 34–38 (E.C.J. May 13, 2014).

³¹⁸ See GDPR, *supra* note 291, at art. 4(8).

[125] As noted above, the personal data stored on a blockchain may consist of metadata and data on the object of each transaction.³¹⁹ The *purposes and means* of processing this personal data can be analysed from two perspectives. On the one hand, at the macro-level, looking at the blockchain infrastructure as a whole, the purpose of processing personal data is to provide the associated service. For instance, with regard to Bitcoin, the purpose of processing transaction data is to provide a peer-to-peer system of electronic cash.³²⁰ At this level, the ‘means’ of processing will generally consist of (i) the software that nodes and miners run to find new blocks and store and update the blockchain database, and (ii) the hardware that nodes and miners use for this purpose.

[126] From this macro-level perspective, nodes and miners arguably decide to engage in processing for their own *purposes*, namely to facilitate the platform. They would also determine the *means* of processing, by deciding which software and hardware to use.

[127] On the other hand, at the micro-level, looking at individual transactions, the *purpose* of the processing is to record a specific transaction onto a blockchain.³²¹ At this level, the *means* would refer to the choice of blockchain platform.

[128] From this micro-level perspective, users enter personal data into the system when submitting their transactions.³²² Thus, for each specific item of personal data, the individual user arguably determines the *purposes* of processing, namely: to record a specific transaction onto the blockchain. The user also determines the *means*, namely: to use that blockchain platform to execute their transaction. From this perspective,

³¹⁹ See discussion *supra* Section 6.2.1.

³²⁰ See Nakamoto, *supra* note 34, at 1.

³²¹ See *id.*

³²² See *id.* at 6.

nodes and miners simply facilitate access to a blockchain database, while the users determine which data are stored there.

[129] In many cases, the analysis of who *determines the purposes and means of processing* will depend on whether you adopt the macro- or micro-level perspective. Since data protection law is concerned with the processing of specific items of personal data, we consider the micro-level perspective more appropriate. To illustrate this point, we consider three different use cases below.

i. Centralised Platform: Land Registry

[130] With a centralised platform, the platform operator will be likely to determine the *means* of processing at the macro-level. For instance, with a land registry, the government agency setting up the platform could either develop the underlying software in-house, or buy in software from a third-party developer. The agency could then run a single node and miner, acting as a TTP. Similarly, at the macro-level, the agency would decide to process personal data on a blockchain platform for the purpose of providing a registry of titles to land. Seen from the macro-level, one could argue that the land registry should be considered a controller.

[131] However, the micro-level perspective instead focuses on individual transactions. The personal data processed on a land registry blockchain would be metadata: in this case, the sender and recipient's identifiers. Users enter this personal data onto the platform for their own purposes, namely to register and/or transfer titles to land. Users also arguably determine the means of processing by choosing the blockchain-based land registry as the medium to execute their transfers. Once users have submitted transactions, the government agency may merely process associated data on the users' behalf. Seen from this micro-level perspective, the user should arguably be considered the data controller, with the agency acting only as a processor on their instructions.

[132] In practice, the government agency need not perform the processing itself, but may engage a sub-processor. For instance, it might

use a Blockchain-as-a-Service (BaaS) offering, whereby a third party provides the underlying supporting infrastructure. The agency could pay a third party to run the miner and node on the third-party's own hardware. In such cases, the BaaS-provider could qualify as a sub-processor when processing personal data for the land registry.

[133] It is important to note, however, that there may be multiple data controllers in relation to a particular set (or subset) of personal data. For example, even if we categorise the government agency running the blockchain land registry platform as a *mere processor* for the purpose of individual transactions, it may nevertheless be a controller for other purposes such as assessment and collection of taxes relating to land transactions.

ii. Closed, Permissioned Platform: Inter-Bank Customer Data Sharing

[134] As a second example, assume a group of parties decide to set up a closed, permissioned blockchain platform with a small number of trusted nodes. For instance, a group of retail banks may set up a blockchain to share information on their customers for KYC purposes. The platform is closed (only the founding banks, or others they authorise, can use it) and private (only the participating banks can view the blockchain database).

[135] At the macro-level, the parties who set up the platform would determine the means of processing by designing the platform. Thus, in specifying the software, the banks would determine which data to store on the blockchain and how it is processed through the consensus protocol. They could also dedicate resources to running the nodes. The banks also arguably determine the purpose of processing, namely to share KYC information. Seen from this perspective, the banks could be characterised as controllers when setting up the platform and when acting as nodes and miners.

[136] However, as above, the micro-level perspective would instead focus on individual transactions. In this case, the personal data would be

the object of the transactions (namely: the customer records). Banks enter this information onto the platform when submitting transactions. In line with the above analysis, as users, each bank would arguably act as a controller with regard to the customer data it submits to the platform. Further, when processing the data as nodes and miners, the banks might be acting only as processors with regard to the customer data that other participating banks have submitted.

[137] The above applies so long as the group of banks acting as nodes/miners only process the transaction data for the purposes determined by the sending user (namely to execute the transaction). If they engage in further processing of the data for their own purposes, they would likely become controllers of that data.³²³ For example, a bank could analyse the customer data stored on its copy of the blockchain to glean commercial insights.

iii. Open, Distributed Platform: Cryptocurrency

[138] For open, distributed platforms, such as Bitcoin, determining controllers and processors is difficult.³²⁴ The definition used by data protection law is arguably ill-suited to distributed platforms, which purposefully lack a central administrator who could bear responsibility for compliance.³²⁵ Instead, control is deliberately distributed.

[139] At the macro-level, the platform's purpose is to facilitate a peer-to-peer system of electronic cash.³²⁶ The means consist of the Bitcoin core software and the hardware provided by nodes and miners. It is generally accepted that these purposes and means were originally envisaged by a

³²³ See Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 8, 01037/12/EN WP 196 (2012) [hereinafter Cloud Computing].

³²⁴ See Finck, *supra* note 297, at 16-18.

³²⁵ See *id.*

³²⁶ See Nakamoto, *supra* note 34, at 1.

person (or persons) known as “Satoshi Nakamoto.”³²⁷ Today, the Bitcoin core code developers control the core software (see Section 3.3 above).³²⁸ This arguably gives them a high degree of factual control over the *why* and *how* of processing Bitcoin transaction data.³²⁹ However, the developers do not process any personal data themselves, unless they also happen to run nodes or mine new blocks.³³⁰ They merely make the software available for others to use.³³¹ As a result, they are unlikely to qualify as either controllers or processors under data protection law.

[140] Nodes and miners process personal data in the form of Bitcoin addresses, for instance when they store and broadcast transaction data.³³² They decide to process such data for the purposes of facilitating the cryptocurrency and, in the case of miners, to reap a reward for mining new blocks.³³³ They provide means in the form of hardware and do so on their own behalf, rather than on instructions from any other party. Given this, the miners and nodes arguably could be controllers.

[141] However, they have limited factual influence over the ‘why’ and ‘how’ of processing. Nodes and miners cannot easily (if at all) change the

³²⁷ See Mitchell Hyman, *Bitcoin ATM: A Criminal's Laundromat for Cleaning Money*, 27 ST. THOMAS L. REV. 296, 298 (2015).

³²⁸ See Christopher, *supra* note 164, at 150.

³²⁹ See Article 29 Working Party, Opinion 1/2010 on the Concepts of “Controller” and “Processor,” 11, 14, 00264/10/EN WP169 (Feb. 16, 2010) [hereinafter *Controller and Processor*].

³³⁰ See Jeffery Atik & George Gerro, *Hard Forks on The Bitcoin Blockchain: Reversible Exit, Continuing Voice*, 1 STAN. J. BLOCKCHAIN L. & POL. 1, 5 (2018).

³³¹ See NISTIR OVERVIEW, *supra* note 6, at 44–45.

³³² See discussion *supra* Section 3.1, 6.2.1.

³³³ See discussion *supra* in Section 3.1.

‘core’ software and its consensus protocol.³³⁴ At most, they can propose changes or move to a different fork.³³⁵ Instead, they download the software and run it passively on their computers.³³⁶ Given this distribution of control, it is not straightforward to identify controllers at the macro-level.

[142] As above, the micro-level perspective focuses instead on individual transactions. The personal data in this case are the sender and recipient’s Bitcoin addresses and (potentially) the related transaction data (e.g. timestamp and amount of BTC). Thus, with respect to each item of personal data, the sending user decides to submit it to the Bitcoin platform for their own purpose, namely to transfer a certain quantity of value to the recipient. In addition, they arguably determine the means of processing, by deciding to use Bitcoin for their transaction. Seen from this micro-level perspective, the users should be considered data controllers. Nodes and miners may simply process this data on behalf of each user.

[143] One could argue that the users have even less factual influence over the means of processing, since they cannot change the Bitcoin software that nodes and miners run.³³⁷ However, this imbalance in power over the means of processing applies to other cases involving individual users and large service providers. For instance, with cloud services, a customer can often only use a commoditised cloud service without modification and may have no choice but to accept the standard contractual terms offered by a large cloud service provider if they wish to use a particular service.³³⁸ Nonetheless, as controllers, the customers

³³⁴ See discussion *supra* in Section 3.3; see also Finck, *supra* note 297, at 17.

³³⁵ See discussion *supra* in Section 3.3.

³³⁶ See discussion *supra* in Section 3.3.

³³⁷ See discussion *supra* in Section 3.3.

³³⁸ See Simon Bradshaw, Christopher Millard, Ian Walden, *Standard Contracts for Cloud Services*, in CLOUD COMPUTING L. (Christopher Millard ed., 2013).

remain responsible for their decision to use a certain service. They should choose a cloud provider that guarantees compliance with the relevant requirements of data protection law.³³⁹ Similarly, cryptocurrency users should arguably choose a platform that is compliant with data protection law.

[144] Nonetheless, some users may benefit from an exemption for personal activities. EU data protection law does not apply to natural persons in the course of a purely personal or household activity.³⁴⁰ Thus, if a group of friends use a cryptocurrency like Bitcoin to make payments to each other, they may be exempt from data protection law in relation to such processing. However, if a user makes payments outside of a personal or household activity, such as for commercial, political, or charitable purposes, the exemption may not apply.³⁴¹ Further, the exemption would be unlikely to apply to legal persons who make Bitcoin payments. In such circumstances, users will typically be subject to the full responsibilities of a data controller, as set out in Section 6.2.3 below.

[145] Finally, anybody who accesses the data stored on a public blockchain and processes it for their own purposes becomes a data controller. Thus, if a node analyses the payments data in its local copy of the blockchain to glean commercial insights, it would become a controller in respect of any personal data involved.

iv. Conclusions Regarding Data Controllers and Processors

[146] In each of the above examples, the characterisation of participants as controllers and/or processors depends on whether a blockchain use case is analysed from the macro- or micro-level perspective. Given that data protection law is concerned with the processing of specific items of

³³⁹ See Cloud Computing, *supra* note 323, at 8.

³⁴⁰ GDPR, *supra* note 291, at art. 2(2)(c).

³⁴¹ See Cloud Computing, *supra* note 323, at 8, 10.

personal data, the micro-level perspective is arguably a more appropriate starting place. Following this line of reasoning, users would be considered data controllers in respect of the personal data they submit to the blockchain platform, since they determine both purposes (to execute the transaction) and means (in choosing the platform). They delegate decisions on the technical and organisational details of the processing to the collective of developers, nodes, and miners.

[147] Whether nodes and miners should also be deemed controllers would depend on the facts of each case. If nodes and miners merely process transaction data on behalf of users, they might merely be processors, rather than controllers. In some cases, they may simply facilitate the processing of transactions on behalf of users, by passively running the relevant software. In this respect, they could be compared to providers of cloud computing services. Cloud providers offer Internet-based, flexible, location-independent access to computing resources, including processing capability and storage.³⁴² In many cases, the cloud customer acts as the data controller, with the cloud provider merely processing the data on their behalf.³⁴³ Similarly, a blockchain-based platform provides access to a distributed application for processing and storing transaction records.³⁴⁴ Just like cloud providers, nodes and miners who provide users with access to hardware and applications are likely to be processors with regard to the personal data submitted by users.³⁴⁵

[148] If, however, nodes and miners take a more active role with regard to the transaction data, they may also be deemed to be controllers. In that case, nodes and miners could be compared to SWIFT, a financial messaging service that facilitates international money transfers for

³⁴² See W. Kuan Hon & Christopher Millard, *Cloud Technologies and Services*, in CLOUD COMPUTING L. (Christopher Millard ed., 2013).

³⁴³ See Cloud Computing, *supra* note 323, at 7–8.

³⁴⁴ See Singh & Michels, *supra* note 190, at 3–4.

³⁴⁵ See generally Hon et al., *supra* note 295.

financial institutions.³⁴⁶ In doing so, SWIFT processes personal data such as the names of payers and payees.³⁴⁷ SWIFT initially presented itself as a mere processor, relaying messages on behalf of the financial institutions. However, the Article 29 Working Party determined that SWIFT should be considered a controller, since it acted with a significant level of autonomy in relation to the personal data it processed, including by developing, marketing, and changing the services it offered, deciding to establish a data centre in the US and to disclose data to the US Treasury.³⁴⁸ Thus, the more autonomy and *effective margin of manoeuvre* the nodes and miners have in respect of the personal data they process, the more likely they are to be considered controllers.

6.2.3 Can Blockchain Controllers and Processors Comply with Data Protection Law?

[149] The uncertainty around the status and roles of controllers and processors complicates many aspects of data protection compliance, including in particular the following:

i. Lawful Grounds for Processing

[150] First, controllers need a lawful ground for processing personal data.³⁴⁹ Processors do not need to establish independently that the controller has valid grounds for processing.³⁵⁰

³⁴⁶ See Article 29 Data Protection Working Party, Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) 01935/06/EN WP128, 2 (2006) [hereinafter SWIFT].

³⁴⁷ See *id.*

³⁴⁸ *Id.* at 11.

³⁴⁹ GDPR, *supra* note 291, at art. 6. (listing of several grounds including, *inter alia*, (i) data subject consent; or that processing is necessary for compliance with (ii) a contract to which the data subject is party; (iii) the controller's legal obligation; or (iv) for legitimate interests the controller is pursuing, provided that the controller's interests are not "overridden by the interests, fundamental rights and freedoms of the data subject").

[151] We argue above that users of blockchain platforms are likely to be deemed controllers. Consequently, unless covered by the household exemption (or another exemption),³⁵¹ each user will need to be able to demonstrate one or more lawful grounds for processing the personal data they submit to the blockchain. For instance, in the above banking example, each bank will need to determine whether its existing grounds for processing customer data extend to processing by means of a private, permissioned blockchain. Further, users of distributed, public platforms such as Bitcoin need to have a legal basis for processing the recipient's address (unless they are covered by the household exemption).³⁵² It could be argued that, in signing up for a Bitcoin address, a recipient has implicitly consented to the processing of that address for transaction purposes.

[152] Conversely, we argue that miners and nodes may be deemed *mere processors*, provided they don't also process personal data for their own purposes (for which they would then need a justification). As a result, they would not normally need to verify whether the controller has valid grounds for processing.

ii. Controller and Processor Obligations

[153] Second, joint controllers must determine their respective responsibilities for compliance by means of an arrangement between them.³⁵³ Further, controllers must put in place a contract with processors

³⁵⁰ *See id.* at art. 28 (3). That said, if, in their opinion, the instructions they receive from controllers infringe the GDPR, processors may be under an obligation to inform the controller accordingly.

³⁵¹ *E.g., id.* at arts. 85, 89.

³⁵² *See, id.* at arts. 6, 85, 89.

³⁵³ *See id.* at art. 26.

to determine how personal data will be processed, including the subject-matter, duration, nature, and purpose of the processing.³⁵⁴

[154] Thus, for each platform, the (joint) controller(s) and processor(s) must establish contractually their data protection responsibilities amongst themselves. Achieving this should generally be easier with closed, centralised platforms, since fewer parties are involved as nodes and miners, making it easier to coordinate compliance. For instance, in the above banking example, the banks would need to establish their respective responsibilities by means of a contract. Similarly, the land registry would need to establish its legal responsibilities as a processor via contracts with the users of its platform. It would probably seek to do so by requiring users to agree to terms of service before accessing the platform.

[155] For open, distributed platforms, it is unclear how controllers and processors might comply with these obligations. In theory, large numbers of users, nodes, and miners would need to enter into detailed contracts in order to establish their responsibilities. In practice, the most feasible way to achieve this may be through standard-form terms and conditions to be agreed whenever a user, node, or miner first uses a platform. These terms would set out the parties' legal obligations.

[156] However, this raises the question as to who will draw up the terms and conditions. As noted above in Section 3.3.1, the platform's software developers are the only closed, centralised layer in Bitcoin (as is the Ethereum Foundation for Ethereum).³⁵⁵ As a result, they are best-positioned to coordinate compliance by designing the platform such that only those who accept the relevant terms and conditions are able to join it. However, as argued above in Section 6.2.2, developers are not controllers or processors in relation to transaction data and are therefore not subject to the contractual requirements of the GDPR. Nonetheless, developers have

³⁵⁴ See GDPR, *supra* note 291, at art. 28.

³⁵⁵ See Christopher, *supra* note 164, at 150.

an interest in promoting their platform and may find that designing it to enable compliance attracts more miners, nodes, and users.

[157] Thus, software developers could require nodes and miners to agree to contractual terms when downloading or updating the relevant software. For example, the Ethereum website contains standard-form terms and conditions governing the use of its software platform, the Bitcoin Core website does not.³⁵⁶ That said, Ethereum's terms do not cover data protection compliance.³⁵⁷ Further, users would need to agree to contractual terms when joining the service through the user interface. However, this is difficult for Bitcoin and Ethereum, since users need not interact with the software directly.³⁵⁸ Instead, user-facing intermediaries (such as wallets and exchanges) would need to require users to agree to a platform's terms and conditions during sign-up.

[158] In addition, the GDPR imposes conditions on transfers of personal data from the EU to *third countries*, i.e. any country outside the EEA.³⁵⁹ Thus, controllers must ensure they have an appropriate legal basis for any international data transfer to a third country. Returning to our earlier examples, in order to run a node in a third country, the land registry and banks would need to ensure an adequate level of protection or appropriate safeguards (for instance by locating the node in a country subject to a Commission adequacy decision or by putting in place adequate safeguards such as via approved standard contract clauses).

³⁵⁶ *Compare Legal Agreement*, ETHEREUM, <https://www.ethereum.org/agreement> [<https://perma.cc/73LT-UMXL>], *with About*, BITCOIN CORE, <https://bitcoincore.org/en/about/> [<https://perma.cc/6NDB-XV4F>].

³⁵⁷ *See Legal Agreement*, ETHEREUM, <https://www.ethereum.org/agreement> [<https://perma.cc/3L4D-93W4>].

³⁵⁸ *See* Kevin D. Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, BERKELEY TECH. L.J. (forthcoming 2018) (manuscript at 27).

³⁵⁹ *See* Hon et al., *supra* note 295. *See generally* GDPR, *supra* note 291, at ch. V.

[159] However, open, distributed platforms are by design unconstrained by international borders: typically anybody, anywhere, can download the entire transaction archive and start processing new transactions as a node or miner.³⁶⁰ As a result, use of these platforms is likely to entail data transfers to third countries. Since any party in any third country can download the archive, adequacy decisions and appropriate safeguards (including binding corporate rules) are unlikely to provide sufficient coverage. Since implicit consent does not suffice for international transfers, the platform's terms of use would need to provide for explicit user consent.³⁶¹

iii. Data Subject Rights

[160] Third, data subjects have rights in respect of their personal data. These include a right to rectification of inaccurate personal data and to data erasure (also known as the *right to be forgotten*).³⁶² At first glance, these rights appear to run counter to blockchain technology's 'immutability'. However, the ability to comply with such requests differs, depending on the design of the blockchain platform.

[161] Centralised platforms can support reversibility better and can limit visibility of a record to certain parties (see Sections 0 and 0 above).³⁶³ As a result, they would be in a better position to comply with data subjects' requests to rectify or erase data in past blocks. For example, if a user requested the banks to rectify a specific piece of information in their customer record on the blockchain, each bank could comply by altering the relevant transaction record and re-hashing the subsequent blocks in

³⁶⁰ See Finck, *supra* note 297, at 18–19.

³⁶¹ See GDPR, *supra* note 291, at art. 49 (1)(a) (indicating “explicit consent” as one of various “derogations” from the data transfer restrictions).

³⁶² See *id.* at arts. 16–17.

³⁶³ See Buterin, *Public and Private Blockchain*, *supra* note 138.

their copy of the ledger. Operators of centralised platforms should similarly be able to comply with requests for erasure.

[162] For open, distributed platforms, it is unclear how individual participants at the user, node or miner level would comply with such requests. A node can only alter its own local copy of the ledger.³⁶⁴ Thus, even if all users, nodes, and miners were considered controllers, this would not necessarily provide effective protection for data subjects.³⁶⁵ In theory, all nodes could agree by contract to ‘fork’ to a new version of the blockchain periodically, to reflect requests for rectification or erasure. However, in practice, this level of coordination may be difficult to achieve among potentially thousands of nodes.

[163] Beyond altering the chain, there may also be other technical approaches to assist data protection compliance. For instance, a blockchain application might not require storage of personal data on-chain, but rather provide links to such data residing externally.³⁶⁶ Therefore, implementing mechanisms that allow deletion of data (despite a link persisting on a block) may be enough to satisfy a request for erasure; so too might deleting all instances of a private key for encrypted data (be it stored on- or off-chain), so as to make that data inaccessible. Technical approaches targeting data protection issues are an active area of research and they are likely to receive an additional impetus due to legal obligations to demonstrate *data protection by design*.³⁶⁷

³⁶⁴ See discussion *supra* Section 3.1.

³⁶⁵ See Matthias Berberich & Malgorzata Steiner, *Blockchain Technology and the GDPR—How to Reconcile Privacy and Distributed Ledgers?*, 2 EUR. DATA PROT. L. REV. 424, 426 (2016).

³⁶⁶ See Guy Zyskind, et al., *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, 2015 IEEE SEC. & PRIVACY WORKSHOPS 180, 181 (2015).

³⁶⁷ See GDPR, *supra* note 291, at art. 25.

iv. Liability

[164] This preliminary analysis illustrates the significant uncertainty as to how EU data protection law might apply to blockchain applications and in particular to open, distributed blockchain platforms. Given the potential severity of penalties under the GDPR, there is a risk that this legal uncertainty will have a chilling effect on innovation, at least in the EU and potentially more broadly. For example, if all nodes and miners of a platform were to be deemed joint controllers, they would have joint and several liability, with potential penalties under the GDPR of up to EUR 20 million or 4% of global turnover/revenues, whichever is higher.³⁶⁸

[165] As a result, it might be helpful if the Article 29 Working Party, or its successor body under GDPR, the European Data Protection Board, were to issue guidance regarding the application of data protection law to various common blockchain models. At a national level, as part of its Information Rights Strategic Plan 2017-2021, the UK Information Commissioner's Office has launched a programme to fund research into the privacy implications of various new technologies, including blockchain.³⁶⁹

6.3 Initial Coin Offerings and Securities Law

[166] An initial coin offering (ICO)—or *token sale*—is a way for a start-up with a new blockchain-based service to raise money by selling an initial set of tokens.³⁷⁰ The company then uses the money raised to launch the service.³⁷¹ Purchasers of the coins or *tokens* can then *spend* their

³⁶⁸ See *id.* at art. 83.

³⁶⁹ See *Grants Programme 2018*, INFO. COMMISSIONER'S OFF. (2018), <https://ico.org.uk/about-the-ico/what-we-do/grants-programme-2018/> [<https://perma.cc/VLQ4-YMHA>].

³⁷⁰ See Jin Enyi & Ngoc Dang Yen Le, *Regulating Initial Coin Offerings* (“*Crypto-Crowdfunding*”), 8 J. INT'L BANKING & FIN. L. 495 (2017).

³⁷¹ See *id.*

tokens to access the service or sell them on cryptocurrency exchanges.³⁷² Many ICO-tokens are built through smart contracts on top of the Ethereum blockchain. ICOs raised an estimated U.S. \$5.5 billion in 2017.³⁷³

[167] Purchasing tokens in an ICO is a high-risk activity.³⁷⁴ Many companies offering ICOs provide investors with little more than a whitepaper and a website.³⁷⁵ If the service proves popular, the tokens' value can increase dramatically. Conversely, if the start-up fails to launch a valuable service, the tokens may become worthless, leaving investors with losses. For example, the terms of the Status ICO, which raised over U.S. \$100 million in 2017, noted that the development of the Status project may be abandoned for lack of interest from the public, lack of funding, or lack of commercial success.³⁷⁶ The recent management battle at Tezos, which raised U.S. \$232 million through an ICO in 2017, further illustrates the risk of such early stage investment.³⁷⁷

[168] From a regulatory perspective, the details of the offering are important, particularly the rights associated with the token. Some token

³⁷² See Nathaniel Popper, *An Explanation of Initial Coin Offerings*, N.Y. TIMES (Oct. 27, 2018), <https://www.nytimes.com/2017/10/27/technology/what-is-an-initial-coin-offering.html> [<https://perma.cc/22QG-5XYK>].

³⁷³ McLannahan, *supra* note 2.

³⁷⁴ See Popper, *supra* note 372.

³⁷⁵ See *Initial Coin Offerings: Know Before You Invest*, FIN. INDUSTRY REG. AUTHORITY (Aug. 31, 2017), <http://www.finra.org/investors/alerts/initial-coin-offerings-know-before-you-invest> [<https://perma.cc/U4GT-G69Y>].

³⁷⁶ *SNT Creation and Status Project Creation Conditions: Explanatory Note & Governance Terms*, STATUS, <https://contribute.status.im/status-terms.pdf> [<https://perma.cc/M5V5-27H9>] (referring to § 5, "Risk of abandonment / lack of success").

³⁷⁷ See Maria Terekhova, *What Tezos Crisis Could Mean for the ICO Space*, BUS. INSIDER (Oct. 26, 2017, 9:06 AM), <https://www.businessinsider.com/what-tezos-crisis-could-mean-for-the-ico-space-2017-10?r=UK&IR=T> [<https://perma.cc/47HQ-JN7Y>].

sales may offer investors the opportunity to profit from a company's success by promising them a share of the resulting profits.³⁷⁸ Hacker and Thomale refer to such tokens as *investment tokens*.³⁷⁹ Investment token sales resemble more traditional sales of securities, like Initial Public Offerings (IPOs).³⁸⁰ Unlike IPO investors, however, ICO investors typically do not gain equity in the company and may have very limited ability to influence the company's direction.³⁸¹

[169] In other instances, token sales offer investors the opportunity to use the service once it's launched.³⁸² Hacker and Thomale classify such tokens as *utility tokens*.³⁸³ In such cases, the offer of tokens might appear closer to a pre-launch 'sales' arrangement, similar to other crowdfunding arrangements such as Kickstarter.³⁸⁴ The characterisation of tokens is important, since many jurisdictions seek to protect investors by regulating securities.³⁸⁵ A key means of providing protection is to mandate disclosure by filing a prospectus, so that investors have access to the information

³⁷⁸ See Phillip Hacker & Chris Thomale, *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies Under EU Financial Law*, EUR. COMPANY & FIN. L. REV. (Nov. 22, 2017) (forthcoming) (manuscript at 25), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820## [<https://perma.cc/98D4-FFS6>].

³⁷⁹ *Id.* manuscript at 13.

³⁸⁰ Philipp Maume & Mathias Fromberger, *Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws*, CHI. J. INT'L L. (June 15, 2018) (forthcoming) (manuscript at 4), <https://papers.ssrn.com/sol3/papers.cfm?abstractid=3200037> [<https://perma.cc/WQ7N-R8FJ>].

³⁸¹ Hacker & Thomale, *supra* note 378, manuscript at 11.

³⁸² *See id.* at 12.

³⁸³ *Id.*

³⁸⁴ *See* Enyi & Le, *supra* note 370.

³⁸⁵ *See* Hacker & Thomale, *supra* note 378, manuscript at 14.

they need in order to assess the risk associated with an investment.³⁸⁶ This can help to address the informational asymmetry between potential investors and the investment's promoters.³⁸⁷

[170] The difficulty lies in the fact that ICOs often combine elements of investment and utility tokens. While the tokens can be used to access the service, ICOs may also offer investors the opportunity to profit from a company's success by selling tokens at a profit on secondary markets.³⁸⁸

[171] Regulators have begun to take action in relation to ICOs.³⁸⁹ Whether a particular ICO will be deemed a security may differ per jurisdiction.³⁹⁰ In the US, organisers of an ICO will need to register a prospectus with the Securities and Exchange Commission (SEC) if the ICO qualifies as an 'investment contract' under the so-called Howey Test.³⁹¹ Under this four-step test, an ICO will qualify as an investment contract if it consists of: (i) an investment of money, (ii) into a common enterprise, (iii) with the reasonable expectation of profits (iv) derived from the entrepreneurial or managerial efforts of others.³⁹²

³⁸⁶ *See id.*

³⁸⁷ *See* Werbach, *supra* note 71, manuscript at 29.

³⁸⁸ *See* Hacker & Thomale, *supra* note 378, manuscript at 13; Jay Clayton, SEC Chairman, *Statement on Cryptocurrencies and Initial Coin Offerings* (Dec. 11, 2017), <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11> [<https://perma.cc/7BAE-7QGT>].

³⁸⁹ *See, e.g.*, Hacker & Thomale, *supra* note 378, manuscript at 5–6; *see also* Clayton, *supra* note 390.

³⁹⁰ *See* Hacker & Thomale, *supra* note 378, manuscript at 6–7.

³⁹¹ *See* SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946); *see also* Hacker, & Thomale *supra* note 380, manuscript at 17–18.

³⁹² *See* W.J. Howey Co., 328 U.S. at 301; *see also* Hacker, & Thomale *supra* note 378, manuscript at 18.

[172] The SEC applied this test to two ICOs in July and December 2017. It determined that ICO tokens can qualify as securities, depending on the facts of the case.³⁹³ In the specific case of *The DAO* (as set out in Section 6.6), the SEC deemed the tokens securities and found that their unregistered sale violated securities regulations.³⁹⁴ In this respect, the SEC considered that *The DAO*'s promotional materials and communications gave investors the reasonable expectation of profits through a return on investment from projects that *The DAO* funded.³⁹⁵

[173] Similarly, in the case of Munchee Inc., the SEC ordered the company to cease its token sale since it violated securities law, noting (inter alia) that token purchasers had a reasonable expectation of profits from their investment in the Munchee enterprise.³⁹⁶ In this respect, the SEC reviewed Munchee's marketing materials including its White Paper, website, a blog post, and statements on a podcast and in various social media.³⁹⁷ It concluded that although Munchee did not offer a dividend or other periodic payment, its communications raised reasonable expectations that purchasers could profit from the appreciation of value of tokens resulting from Munchee's efforts to develop its business.³⁹⁸

³⁹³ See Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 (July 25, 2017) [hereinafter DAO Report]; see also Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, Making Findings, and Imposing a Cease-and-Desist Order, Release No. 10445 (Dec. 11, 2017) [hereinafter Munchee Order].

³⁹⁴ See DAO report, *supra* note 393, at 1–2.

³⁹⁵ See *id.* at 11–12.

³⁹⁶ See Munchee Order, *supra* note 393, at 1, 6.

³⁹⁷ See *id.* at 3.

³⁹⁸ See *id.* at 9.

[174] The UK Financial Conduct Authority has also announced that ICOs would, under certain circumstances, be regulated as securities.³⁹⁹ Under EU law, organisers of an ICO will need to register a prospectus if the ICO qualifies as a security. Failure to do so can give rise to significant civil and criminal liability.⁴⁰⁰ Under the EU Prospectus Regulation,⁴⁰¹ an ICO will qualify as a security if the issued units are (i) transferable, (ii) negotiable, (iii) standardised (meaning they must be easily traded on a capital market), and (iv) functionally similar to shares, bonds, or other forms of securitized debt.⁴⁰² Hacker and Thomale argue that under this test, ICOs should be considered securities if the organisers' promotional materials and other communications raise investor expectations of profits.⁴⁰³ This could be the case, for example, if these materials highlight the possibility of trading tokens on secondary markets.⁴⁰⁴ Conversely, a pure *utility token* that is focused only on token-holders' claims to redeem a service from the issuer (and that does not raise expectations of profits) might not be subject to security regulation.⁴⁰⁵

[175] It remains to be seen how EU regulators and courts will approach ICOs. Ultimately, regulators will need to consider how to regulate ICOs in

³⁹⁹ See *Initial Coin Offerings*, FIN. CONDUCT AUTHORITY (Dec. 9, 2017), <https://www.fca.org.uk/news/statements/initial-coin-offerings> [<https://perma.cc/WRU3-9DS7>].

⁴⁰⁰ See Hacker & Thomale, *supra* note 378, manuscript at 19.

⁴⁰¹ See generally Commission Regulation 2017/1129, 2017 O.J. (L168/12) (EU) (describing the regulation when securities are offered to the public or admitted to trading on a regular market).

⁴⁰² See Hacker & Thomale, *supra* note 378, manuscript at 20–25.

⁴⁰³ See *id.* at 44 (stating that regulatory laws should apply to currency and utility tokens); see also DAO Report, *supra* note 393, at 11–12; Munchee Order, *supra* note 393.

⁴⁰⁴ See Hacker & Thomale, *supra* note 378, manuscript at 33.

⁴⁰⁵ See *id.* manuscript at 28–30.

order to protect investors without chilling innovation.⁴⁰⁶ In the long-term, appropriate regulation should bolster these new ways of fundraising. Without protection, investors risk being misinformed and suffering losses, which in turn is likely to undermine confidence in the market as a whole.⁴⁰⁷

6.4 Digital Tokens and Property Law

[176] Blockchains track transactions in digital tokens between users. As noted above in Section 2.2, users exercise control over their tokens through their private keys. Although tokens often have financial value, it is not clear to what extent they qualify as *property* under the law. This section considers the status of blockchain tokens under the property law of England and Wales.⁴⁰⁸

[177] The answer may have significant practical implications. For example, crypto-currency holdings have given rise to disputes in divorce cases, where a court can order the transfer or sale of a party's property.⁴⁰⁹ The property status of tokens will likely prove relevant to other legal areas that use definitions of property as well, including the law of torts (e.g. the

⁴⁰⁶ See Peter Van Valkenburgh, *Framework for Securities Regulation of Cryptocurrencies*, COIN CTR. REP. 59–60 (Aug. 10, 2018), <https://coincenter.org/entry/framework-for-securities-regulation-of-cryptocurrencies> [<https://perma.cc/Z3Y5-ZZ2N>].

⁴⁰⁷ See Werbach, *supra* note 71, manuscript at 30.

⁴⁰⁸ Since property law is not harmonised at the EU level, we have chosen to analyse this question under a national law.

⁴⁰⁹ See Matrimonial Causes Act, 1973, c. 18, pt. 2, §§ 24(1), 25(2)(a) (Eng. & Wales). See generally Muhammad Sarfaraz, *Bitcoin, Ripple and Other Cryptocurrency Assets Are Now Part of Divorce Settlements*, LINKEDIN (Feb. 15, 2018), <https://www.linkedin.com/pulse/bitcoin-ripple-other-cryptocurrency-assets-now-part-divorce-muhammad/> [<https://perma.cc/9UTD-322J>] (stating that cryptocurrencies are a significant part in divorce settlements).

tort of conversion), bankruptcy law,⁴¹⁰ succession law,⁴¹¹ and the criminal offence of theft.⁴¹² For example, imagine a third party gains access to a crypto-currency user's private key and sends tokens to another account. Might that constitute theft? Alternatively, in future bankruptcy cases, a debtor may hold an amount of crypto-currency of significant value. Could a court order the tokens be sold to repay creditors?

[178] While the questions may seem simple, the legal classification of blockchain tokens is complicated. Further, whether tokens qualify as property may depend on the legal context and the remedy sought, since an item might qualify as property in some contexts but not in others.⁴¹³ For example, the Theft Act 1968 has a specific definition of *property*.⁴¹⁴ Nonetheless, the section below provides an overview of the general arguments that could be raised to determine the property status of tokens in a specific case.

⁴¹⁰ See Insolvency Act, 1986, c. 45, pt. 9, § 283(1) (Eng. & Wales); Insolvency Act, 1986, c. 45, pt. 18, § 436(1) (Gr. Brit.); David E. Kronenberg & Daniel Gwen, *Bitcoins in Bankruptcy: Trouble Ahead for Investors and Bankruptcy Professionals?*, 10 PRATT'S J. BANKR. L. 112, 116 (2014) (discussing Bitcoin as property in the US bankruptcy context).

⁴¹¹ See Administration of Estates Act, 1925, c. 23, pt. 3, § 32 (Eng. & Wales).

⁴¹² See Theft Act, 1968, c. 60, §§ 1(1), 4(1) (Eng. & Wales); see also Law of Property Act, 1925, c. 20, pt. 12, § 205(1)(xx) (Eng. & Wales).

⁴¹³ See generally Kelvin F.K. Low & Ernie G.S. Teo, *Bitcoins and Other Cryptocurrencies As Property?*, 9 LAW, INNOVATION & TECH. 235, 235 (2017) (discussing whether cryptocurrencies should be considered property and what rights the law should afford them).

⁴¹⁴ See Theft Act, 1968, c. 60, § 4(1) (Eng. & Wales) (stating that property "includes money and all other property, real or personal including things in action and other intangible property).

6.4.1 Tokens as Property

[179] At the outset, transferable property rights can be distinguished from non-transferable personal rights.⁴¹⁵ As Baroness Hale noted in *OBG v Allan*: “[t]he essential feature of property is that it has an existence independent of a particular person.”⁴¹⁶ “[I]t can be bought and sold, given and received,” bequeathed and inherited, and pledged or seized to secure debts.⁴¹⁷

[180] In *National Provincial Bank v. Ainsworth*, the House of Lords had to determine whether a deserted wife had any property right in her husband’s home.⁴¹⁸ The husband had secured a debt from a bank by a charge on the home.⁴¹⁹ Following non-payment of the debt, the bank sought possession of the home.⁴²⁰ Lord Wilberforce concluded that the wife’s right of occupation of her husband’s property was a personal right, enforceable only against her husband.⁴²¹ He proceeded to set out a four-step test to be met “[b]efore a right or an interest can be admitted into the category of property,” namely: it must be (i) definable; (ii) identifiable by

⁴¹⁵ See JAMES PENNER, *The Objects of Property: The Separability Thesis*, in *THE IDEA OF PROPERTY IN LAW* 113 (2000) (arguing that the object of a property right must be separable and distinct from any person, giving rise to alienability); Joanna Perkins & Jennifer Enwezor, *The Legal Aspect of Virtual Currencies*, 31 *BUTTERWORTHS J. INT’L BANKING & FIN. L.* 569, 569–70 (2016).

⁴¹⁶ *OBG v. Allan* [2007] UKHL 21, [406] (emphasis added).

⁴¹⁷ *Id.*

⁴¹⁸ See *Nat’l Provincial Bank v. Ainsworth* [1965] AC 1175.

⁴¹⁹ See *id.* at 2.

⁴²⁰ See *id.*

⁴²¹ See *id.* at 19–20.

third parties; (iii) capable in its nature of assumption by third parties; and (iv) have some degree of permanence or stability.⁴²²

[181] In *Armstrong v. Winnington Networks*, Stephen Morris QC sitting as deputy High Court judge applied this four-step test to an EU allowance (EUA) to emit carbon dioxide.⁴²³ In this case, the defendant, a German company, had purchased EUAs from a third party, who had fraudulently obtained them from the claimant.⁴²⁴ The claimant, a UK trader in EUAs, brought a claim of proprietary restitution against the defendant.⁴²⁵ Stephen Morris QC concluded that the EUA met the four-step test, since it (i) could be defined as the sum total of rights and entitlements conferred on the holder under the Emissions Trading Scheme legislation (ETS); (ii) was identifiable through its unique reference number; (iii) was transferable under ETS; and (iv) had permanence and stability through entries on the registry. Consequently, it was property at common law.⁴²⁶

[182] It seems likely that many tokens on blockchain-based applications will also satisfy this test.⁴²⁷ They can be defined as the right to control the token; are identifiable through entries on the blockchain; can be transferred by submitting transactions; and are registered with a high degree of permanence and stability.⁴²⁸ This suggests that holders of digital tokens could have a property interest under common law.

⁴²² *See id.* at 20.

⁴²³ *See Armstrong DLW GmbH v. Winnington Networks* [2012] EWCH (Ch) 10, [7].

⁴²⁴ *See id.* at 425.

⁴²⁵ *See id.*

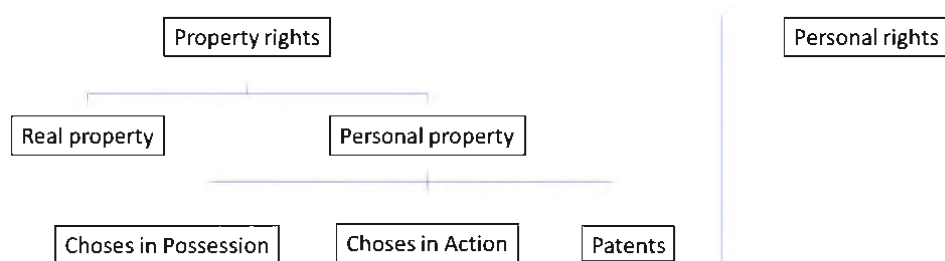
⁴²⁶ *See id.* at 426.

⁴²⁷ *See George Walker, Financial Technology Law—A New Beginning and a New Future*, 50 INT'L LAW 137, 205 (2017).

⁴²⁸ *See id.* at 206.

[183] However, classifying that property interest is more difficult.⁴²⁹ Common law distinguishes between real property (land) and personal property (all other property).⁴³⁰ Personal property is traditionally further split into choses in possession and choses in action.⁴³¹ Patents are granted a separate property status by law as a form of personal property without being a chose in action.⁴³²

Figure 4. Overview of Property Rights in England and Wales



6.4.2 Tokens as Choses in Possession

[184] Choses in possession are tangible things of which a person may have physical possession and which are capable of transfer by delivery.⁴³³ Since digital tokens do not exist in physical form, they would not qualify

⁴²⁹ See *id.* at 205.

⁴³⁰ See ROGER J. SMITH, PROPERTY LAW 8 (8th ed. 2014); see also MICHAEL BRIDGE, PERSONAL PROPERTY LAW 10 (4th ed. 2015).

⁴³¹ See BRIDGE, *supra* note 430, at 12; SMITH, *supra* note 430, at 8.

⁴³² See Patents Act 1977 c. 37, pt. 1, § 30(1) (UK). See generally BRIDGE, *supra* note 430, at 14 (stating that patents are in a select group in which their intangible property rights are greater than their tangible ones).

⁴³³ See BRIDGE, *supra* note 430, at 12.

as choses in possession.⁴³⁴ However, Green and Randall have argued that the law should recognise that the essential elements of possession can be exercised over digital assets that bear the characteristics of excludability and exhaustibility.⁴³⁵ Tokens are susceptible to exclusive access, control, transfer, and loss through the associated private key, in a manner functionally similar to things in physical possession.⁴³⁶ This could argue in favour of recognising a digital token as a chose in *virtual possession* or as a further form of *intangible property* that is capable of possession.⁴³⁷

[185] However, case law militates against recognizing possession of digital assets. In *Your Response v. Business Media*, the Court of Appeals sought to determine whether an electronic database was a form of property capable of possession, such that it could be subject to a possessory lien.⁴³⁸ Lord Justice Moore-Bick held that while Green and Randall made a powerful case, the course they proposed departed significantly from existing case law.⁴³⁹ He did not consider this course open to the court, which may have to await the intervention of Parliament.⁴⁴⁰ In *Armstrong v. Winnington Networks*, Stephen Morris QC reached a similar

⁴³⁴ See generally *Personal Property*, (2013), § 3, 80 HALS. STAT. (5th ed.) 801, 834 (distinguishing physical and legal possession).

⁴³⁵ See SARAH GREEN & JOHN RANDALL, *THE TORT OF CONVERSION* 120 (2009).

⁴³⁶ See Perkins & Enwezor, *supra* note 415, at 569–70.

⁴³⁷ See *id.* at 570.

⁴³⁸ See *Your Response v. Datateam Business Media* [2014] EWCS (Civ) 281 (Eng.).

⁴³⁹ See *id.* at [27].

⁴⁴⁰ See *id.*

conclusion.⁴⁴¹ While recognising that an EUA could be considered similar to a chose in possession, Stephen Morris QC held that the current state of the law did not allow for a conclusion that a thing, which existed only in electronic form could be the subject of actual possession.⁴⁴²

[186] Given the above, it is unlikely that a court in England and Wales would recognise a digital token as a chose in possession. Instead, it seems likely that legislation would be required to introduce a new category of *choses in virtual possession*.⁴⁴³ Doing so would arguably provide a degree of functional equivalence between digital and physical assets.⁴⁴⁴ However, as Lord Justices Davis and Floyd warned in *Your Response v. Business Media*, extending possession to intangible items could have significant unintended consequences,⁴⁴⁵ particularly given the many contexts in which a definition of property applies and the various types of digital assets which could be subject to virtual possession. A full discussion of this issue is beyond the scope of this paper. The issue would likely benefit from further research.

⁴⁴¹ Compare *Your Response V. Datateam Business Media* [2014] EWCS (Civ) 281, [27] (“to take the course which they propose would involve a significant departure from the existing law), with *Armstrong DLW GmbH v. Winnington Networks* [2012] EWHC (Ch) 10, [51] (Eng.) (stating that “the current state of the law has not developed to the point where something which exists in electronic form only is to be equated with a physical thing of which actual possession is possible.”).

⁴⁴² See *Armstrong DLW GmbH v. Winnington Networks* [2012] EWHC (Ch) 10, [51] (Eng.).

⁴⁴³ See Walker, *supra* note 427, at 206.

⁴⁴⁴ See GREEN & RANDALL, *supra* note 435, at 131.

⁴⁴⁵ See *Your Response v. Datateam Business Media* [2014] EWCS (Civ) 281, [41] (Eng.).

6.4.3 Tokens as Choses in Action or “Other Intangible Property”

[187] Choses in action covers all personal rights of property relating to intangible items which can only be claimed or enforced by legal action (and not by taking physical possession).⁴⁴⁶ This category covers various kinds of property including debts, rights under contract, and shares, as well as various forms of intellectual property, e.g. copyright, design rights, and trademarks.⁴⁴⁷ For example, the money a customer stores with a bank is a chose in action.⁴⁴⁸ The customer deposits money and the bank owes the customer a debt. The debt is a right of action that can be transferred to other persons.⁴⁴⁹

[188] Whether a digital token will constitute a chose in action is likely to depend on the circumstances of the particular case and in particular whether the token represents a specific right against the issuer. In some cases, a token may represent a right that is substantially similar to an existing chose in action, such as a debt or share in the issuing company. In such cases, the token is likely to qualify as a chose in action. It arguably functions like a digital version of a *documentary intangible*, like a cheque or a bill of lading; where a physical document represents an intangible chose in action.⁴⁵⁰ Such tokens further resemble a *transferable document or instrument* contained in a reliable electronic record under the UNCITRAL Model Law on Electronic Transferable Records, which sets

⁴⁴⁶ Choses in Action, (2017) § 1, 13 HALS. STAT. (5th ed.) 1, 1.

⁴⁴⁷ See *id.* at 5–9.

⁴⁴⁸ See SMITH, *supra* note 430, at 4–5; see also BRIDGE, *supra* note 430, at 21.

⁴⁴⁹ See *id.*

⁴⁵⁰ Cf. Perkins & Enwezor, *supra* note 415, at 570.

out model rules for the legal recognition of electronic transferable records “on a technologically neutral basis.”⁴⁵¹

[189] In other cases, as set out above in Section 6.3, digital tokens may be sold as part of an ICO by a particular business and give the user a contractual right against the issuer.⁴⁵² For example, the token may give the holder a right to use a particular service (a so-called *utility token*) or to share in the company’s profits (an *investment token*). In such cases, the tokens are likely to constitute a chose in action, if the counterparty and rights associated with the token are clearly defined. They resemble other forms of non-personal, transferable contractual obligations. The key issue in this respect is not whether the blockchain is centralised or distributed at the level of nodes or miners, but whether the token represents a clear obligation held by users against the developers/issuers. For example, a company could issue special ICO tokens on top of the distributed Ethereum blockchain.

[190] However, not all ICO tokens give purchasers a clear right against the issuer. For example, the terms of the EOS ICO Token Purchase Agreement state explicitly that the tokens have no rights, uses, or attributes.⁴⁵³ Other tokens only give purchasers an undefined right to use a platform that may be launched at some future time.⁴⁵⁴ In such cases, the argument for classifying the token as a chose in action is significantly weaker.

[191] The classification of cryptocurrency tokens is even more difficult. First, unlike several other types of choses in action (e.g. debts), there is no

⁴⁵¹ See *UNCITRAL Model Law on Electronic Transferable Records*, UNITED NATIONS COMM’N INT’L TRADE L. 5, 37–38 (2018).

⁴⁵² See discussion *supra*, Section 6.3.

⁴⁵³ *EOS Token Purchase Agreement*, BLOCK.ONE (Sept. 4, 2017), <https://eos.io/documents/block.one%20%20EOS%20Token%20Purchase%20Agreement%20-%20September%204,%202017.pdf> [<https://perma.cc/HX49-AX4B>].

⁴⁵⁴ See, e.g., *SNT Creation*, *supra* note 376, at 1, 2.

specific counterparty with an obligation.⁴⁵⁵ As set out in Section 2, a Bitcoin does not give rise to any rights against others; it only gives a user the exclusive technical control over an amount of Bitcoin, i.e. entries in the UTXO database.⁴⁵⁶ Further, as set out in Section 3.1 and 3.3, there is no specific issuing party; only a group of core developers who manage the Bitcoin software.⁴⁵⁷

[192] Second, the existing types of choses in action without a specific obligor (like copyright) arise from legislation.⁴⁵⁸ As noted above, in *Armstrong v. Winnington Networks*, Stephen Morris QC determined that an EUA constituted property at common law.⁴⁵⁹ In particular, it was a form of *intangible property*, being either a chose in action or some form of *other intangible property*.⁴⁶⁰ In reaching this conclusion, he applied a three-step test: (i) there must be a statutory framework conferring an entitlement; (ii) the entitlement must be transferable; and (iii) the entitlement must have value.⁴⁶¹ In all existing cases, tokens on distributed blockchain applications lack a legislative framework and will fail the first prong of this test.⁴⁶²

⁴⁵⁵ See Low & Teo, *supra* note 413, at 246.

⁴⁵⁶ See generally Andresen, *supra* note 82 (stating that the UTXO database serves to prohibit double-spending or spending bitcoins that do not exist).

⁴⁵⁷ See Christopher, *supra* note 164, at 150.

⁴⁵⁸ See Noel McGrath, *Transacting in a Vacuum of Property Law* (Transnat'l L. Inst. Think!, Paper No. 22/2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2786206 [<https://perma.cc/7E9K-AFLN>].

⁴⁵⁹ See *Armstrong DLW GmbH v. Winnington Networks* [2012] EWHC 10, [50] (Eng.).

⁴⁶⁰ See *id.* at 442.

⁴⁶¹ See *id.* at 440–41.

⁴⁶² See McGrath, *supra* note 458.

[193] As a result, it is difficult to recognise distributed blockchain tokens as choses in possession or choses in action. On a traditional view, if they are neither choses in possession nor in action, then they are arguably not property at all.⁴⁶³ The question then arises whether tokens could constitute a form of *other intangible property*. However, it is unclear whether the common law as applied in England and Wales recognises a category of *other intangible property* (other than choses in action and patents). On the one hand, in *Armstrong v. Winnington Networks*, Stephen Morris QC appeared open to recognising other forms of intangible property.⁴⁶⁴ Further, the definition of property in the Theft Act 1968 explicitly includes both “things in action” and “other intangible property.”⁴⁶⁵ On the other hand, in *Your Response v. Business Media*, Lord Justice Moore-Bick considered it “very difficult to accept that the common law recognise[d] the existence of *intangible property* other than choses in action,” and patents.⁴⁶⁶

[194] Given the above, the property status of digital tokens on distributed blockchain applications under property law is uncertain.⁴⁶⁷ The classification as either a chose in action or a chose in possession can have significant practical consequences. For example, the tort of conversion is

⁴⁶³ Cf. Ken Moon, *The Nature of Computer Programs: Tangible? Goods? Personal Property? Intellectual Property?*, 31.EUR. INTELL. PROP. REV. 1, 15 (2009) (stating that personal property is either a chose in action or a chose in possession).

⁴⁶⁴ See generally *Armstrong DLW GmbH v. Winnington Networks* [2012] EWHC 10 (Ch), [52]–[60] (Eng.) (analyzing EUA as intangible property by discussing case law).

⁴⁶⁵ See Theft Act, 1968, c. 60, § 4(1) (Eng. & Wales).

⁴⁶⁶ *Your Response v. Datateam Business Media* [2014] EWCS (Civ) 281, [25]–[26] (Eng. & Wales) (emphasis added) (citing Lord Justice Fry’s holding in *Colonial Bank v. Whinney* (1885) 30 Ch. D. 261 that “all personal things are either in possession or in action [and] the law knows no tertium quid between the two,” as upheld in the House of Lords (1886) 11 App. Cas. 426).

⁴⁶⁷ See discussion *supra*, at [193].

only available for choses in possession, not choses in action.⁴⁶⁸ The issue has already arisen before a US court, where a claimant is seeking damages for, or the return of, over 1m BTC under the tort of conversion from a defendant who allegedly wrongfully deprived the claimant of the tokens.⁴⁶⁹ Until the status of such tokens is clarified by case law or legislation, this issue may cause consternation for lawyers and courts in future divorce, bankruptcy, criminal law, and succession cases.

6.5 Blockchain Databases and Intellectual Property Law

[195] Various forms of intellectual property may apply to different aspects of blockchain technology. First, blockchain-related inventions that provide a novel, non-obvious technical solution that is capable of industrial application may be patentable.⁴⁷⁰ The core components of blockchain technology are public knowledge and many developers may opt to share their code freely, using an open-source license.⁴⁷¹ For example, Bitcoin and Ethereum's software are available under various open-source license terms.⁴⁷² Nonetheless, companies are filing patent

⁴⁶⁸ See *OBG, v. Allan*, [2007] UKHL 21, [384] (UK).

⁴⁶⁹ See Alex Hern, *Self-Proclaimed Bitcoin 'Creator' Sued for \$10bn*, *GUARDIAN*, (Feb. 27, 2019, 6:11 PM), <https://www.theguardian.com/technology/2018/feb/27/bitcoin-craig-wright-self-proclaimed-creator-sued-10bn-former-coding-partner-family> [<https://perma.cc/4WSK-NK48>].

⁴⁷⁰ See Tim Press, *Patent Protection for Computer-related Interventions*, in *COMPUTER LAW* (Chris Reed ed., 7th ed. 2012).

⁴⁷¹ Cf. Peter Van Valkenburgh, *What is "Open Source" and Why Is It Important for Cryptocurrency and Open Blockchain Projects?*, *COIN CTR.* (Oct. 17, 2017), <https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects> [<https://perma.cc/ZA5N-TSMT>] (stating that open source software and decentralization is important in blockchain technology).

⁴⁷² See, e.g., *Licensing*, *GITHUB*, <https://github.com/ethereum/wiki/wiki/Licensing> [<https://perma.cc/UL33-296N>]; *MIT License*, *GITHUB*, <https://github.com/bitcoin/bitcoin/blob/master/COPYING> [<https://perma.cc/9QWT-Y52Y>].

applications for improvements to existing blockchain technology, including relating to security and encryption techniques.⁴⁷³ For example, Accenture has reportedly been awarded a patent for its editable blockchain technology.⁴⁷⁴ A patent will grant the right holder exclusive rights to the commercial exploitation of the protected invention.⁴⁷⁵

[196] Second, the information stored on a specific blockchain database could be protected by copyright. Under the EU's 1996 Directive on the legal protection of databases (the Databases Directive), EU member states are required to provide copyright protection for databases, which "by reason of the selection or arrangement" of contents "constitute the author's own intellectual creation."⁴⁷⁶ To attract copyright protection, the author must have expressed his creative ability in an original manner by making free and creative choices in setting up the database.⁴⁷⁷ By contrast, the database will lack the required originality, if the setting up was dictated by technical considerations.⁴⁷⁸ Since the information stored on a blockchain will ordinarily be determined by technical design decisions based on a platform's desired functionality, it seems likely that most blockchain databases will not be protected by copyright under EU law.

⁴⁷³ See *A Rush to Patent the Blockchain is a Sign of the Technology's Promise*, ECONOMIST (Jan. 12, 2017), <https://www.economist.com/news/business/21714395-financial-firms-and-assorted-startups-are-rushing-patent-technology-underlies> [<https://perma.cc/7U9R-FSCH>].

⁴⁷⁴ Stan Higgins, *Accenture Awarded Patent for 'Editable Blockchain' Tech*, COINDESK (Sept. 28, 2017, 9:00 AM), <https://www.coindesk.com/accenture-awarded-patent-editable-blockchain-tech/> [<https://perma.cc/3DFX-MZKZ>].

⁴⁷⁵ See *Rights Granted Under U.S. Patent Law*, BITLAW, <https://www.bitlaw.com/patent/rights.html> [<https://perma.cc/D2FW-F4P4>].

⁴⁷⁶ Directive 96/9, of the European Parliament and of the Council of March 1996 on the Legal Protection of Databases, 1996 O.J. (177) art. 3(1).

⁴⁷⁷ See *id.*

⁴⁷⁸ See Case C-604/10, *Football Dataco v. Yahoo! UK*, 2012 EUR-Lex CELEX LEXIS 115 (Mar. 1, 2012).

[197] Third and finally, a blockchain database could be protected as a database under the Databases Directive's *sui generis* protection right for databases.⁴⁷⁹ This *sui generis* right protects databases for which there has been (qualitatively or quantitatively) a substantial investment in the obtaining, verification, or presentation of their contents.⁴⁸⁰ This right is not affected by making the database publicly accessible.⁴⁸¹

[198] The Database Directive defines a database as “a collection of independent works, data or other materials which are arranged in a systematic or methodical way and individually accessible by electronic or other means.”⁴⁸² As set out in Section 2.1 above, a blockchain uses blocks linked through hash pointers to store transactions records, which can be individually accessed through lookup.⁴⁸³ Given this, many blockchain applications will likely qualify as databases. To qualify for a *sui generis* protection right, there must have been a substantial investment in the creation of the database.⁴⁸⁴ According to the European Court of Justice, an investment in the presentation of the contents of a database concerns “the resources used for the purpose of giving the database its function of processing information, that is to say those used for the systematic or methodical arrangement of the materials contained in that database and the

⁴⁷⁹ See generally Directive 96/9, *supra* note 476 (stating the object of protection, the rights and obligations of lawful users, exceptions to the *sui generis* right, term of protection, and beneficiaries of protection under the *sui generis* right).

⁴⁸⁰ See *id.* at 7.

⁴⁸¹ See Case C-203/02, *British Horseracing Board v. William Hill*, 2004 EUR-Lex CELEX LEXIS 333 (June 8, 2004).

⁴⁸² Directive 96/9, *supra* note 476, at art.1.

⁴⁸³ See discussion *supra* Section 2.1.

⁴⁸⁴ See Case C-338/02, *Fixtures Marketing v. Svenska Spel AB*, 2004 EUR-Lex CELEX LEXIS 696 (Nov. 9, 2004) (holding that “the expression ‘investment in . . . the obtaining, verification or presentation of the contents’ of a database must be understood, generally, to refer to investment in the creation of that database as such.”).

organisation of their individual accessibility.”⁴⁸⁵ It could be argued that the operator(s) of a new, centralised blockchain platform make a substantial investment in setting up the blockchain database. For instance, they might invest in the presentation of the database by deploying human, financial, and technical resources in writing the blockchain software and then dedicating hardware to running nodes and miners.⁴⁸⁶

[199] Nonetheless, it is unclear whether such investments qualify as a substantial investment in the creation of a database. In practice, this may depend on each specific platform’s design and functionality and whether extending protection aligns with the purpose of the *sui generis* right, namely to “promote the establishment of storage and processing systems for existing information.”⁴⁸⁷

[200] Given the above, certain blockchain databases may be protected under the *sui generis* right. If so, and provided they have sufficient links to an EU Member State,⁴⁸⁸ the right holders of a centralised platform would have the right to prevent extraction and re-utilization of (all or a substantial parts of) the contents of that database.⁴⁸⁹ This may be relevant to instances of *forking*, where a third-party takes an existing blockchain database as the basis for starting a new blockchain platform (see Section 3.3 above).⁴⁹⁰

⁴⁸⁵ *Id.*

⁴⁸⁶ *See id.*

⁴⁸⁷ *Id.*

⁴⁸⁸ *See* Directive 96/9, *supra* note 476, at art. 11 (requiring beneficiaries to be nationals of an EU Member State, or have their habitual residence in the territory of the Community, or to be companies and firms formed in accordance with a Member State’s laws with their registered office, central administration, or principal place business within the Community).

⁴⁸⁹ *See id.* at 5, 7.

⁴⁹⁰ *See* discussion *supra* Section 3.3 (discussing forking and starting new blockchain platforms from existing blockchains).

[201] Determining whether there has been a *substantial investment*—and if so who holds the rights - would be more difficult for distributed platforms. The database right is owned by the *maker* of the database, being *the person who takes the initiative and the risk of investing*.⁴⁹¹ However, as set out in Sections 3.1 and 3.3 above, various groups may contribute to the creation of an open, distributed blockchain, with developers writing the initial software, and nodes and miners investing in hardware that stores and updates the database. It is unclear whether these activities, taken separately, amount to *substantial investments*, and if so, which of the activities would suffice for a party to qualify as one of the database *makers*.

6.6 Digital Autonomous Organisations and Company Law

[202] Smart contracts can be used to manage the assets and determine the structure, purposes, and functioning of an organisation, known as a Decentralised Autonomous Organization (DAOs).⁴⁹² For instance, a DAO could have a number of members who could together, say by two-thirds majority, decide how to spend funds. This replicates some of the elements of a legal company, such as dividend-receiving shareholders and tradable shares, but using only smart contracts for enforcement.⁴⁹³ As a result, a DAO could allow strangers to contribute capital towards a common enterprise pseudonymously, without needing to trust a management team to exercise control over the company and its associated capital.

[203] However, most jurisdictions feature formal requirements for creating a company, such as registration with a central registry like the UK's Companies House.⁴⁹⁴ As a result, a DAO might not qualify as a

⁴⁹¹ See Directive 96/9, *supra* note 476, at Recital 41.

⁴⁹² See Buterin, ETHEREUM WHITE PAPER, *supra* note 109, at 1.

⁴⁹³ See *id.* at 23.

⁴⁹⁴ See *Set Up a Private Limited Company*, GOV.UK, <https://www.gov.uk/limited-company-formation> [<https://perma.cc/9ZJN-G7B7>].

recognised *legal person* or offer shareholders limited liability. Participants in a DAO may face significant legal risk, potentially being held personally responsible for the DAO's liabilities.⁴⁹⁵

[204] Further, DAOs suffer from the same risk of human error as smart contracts, as illustrated by the hack of *The DAO* set up on the Ethereum platform. *The DAO* was set up in 2016 as a funding vehicle for Ethereum-based projects, such as using *smart locks* to let people share their physical assets (e.g. cars, boats, apartments).⁴⁹⁶ It attracted over U.S. \$160 million in Ether funding from around 11,000 members.⁴⁹⁷ However, a hacker exploited a vulnerability in *The DAO*'s smart contracts and siphoned off almost a third of its funds.⁴⁹⁸

[205] Since Ethereum is an open, distributed platform, the only way to *correct* the effects of this hack (without the hacker's cooperation) was to convince nodes to replace their local copy of the blockchain with a chain in which the funds were still held by *The DAO*.⁴⁹⁹ In the event, this was achieved and a majority of Ethereum nodes moved to the new chain,

⁴⁹⁵ See Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain* 36 (Univ. New South Wales L. Res. Series, Paper No. 52, 2017), <https://ssrn.com/abstract=3018214> [<https://perma.cc/AZ9L-LZMW>].

⁴⁹⁶ See Giulio Prisco, *Slock.it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy*, BITCOIN MAG. (Nov. 5, 2015, 1:05 PM), <https://bitcoinmagazine.com/articles/slock-it-to-introduce-smart-locks-linked-to-smart-ethereum-contracts-decentralize-the-sharing-economy-1446746719/> [<https://perma.cc/R6JK-9LLJ>]; cf. Falkon, *supra* note 501 (“members of the Ethereum community announced the inception of The DAO, which was also known as Genesis DAO. It was built as a smart contract on the Ethereum blockchain.”).

⁴⁹⁷ See Voshmgir Shermin, *Disrupting Governance with Blockchains and Smart Contracts*, in 26 THE FUTURE OF MONEY AND FURTHER APPLICATIONS OF THE BLOCKCHAIN 499, 506. (2017).

⁴⁹⁸ See *id.*

⁴⁹⁹ See discussion *supra* Section 3.3.2.

thereby reversing the attack.⁵⁰⁰ A minority of users refused to do so and stayed on the original branch, which was renamed “Ethereum Classic.”⁵⁰¹ However this was a particularly high-profile, one-off incident, affecting a large number of participants. Such contentious hard forks may be unlikely for issues affecting fewer parties or deemed by the community as insignificant compared with the cost of implementing a fork.

[206] As noted above, centralised platforms support reversibility better.⁵⁰² A single TTP or group of trusted nodes can revert transactions and modify balances if necessary, for instance to enforce court decisions.⁵⁰³

IV. CONCLUSIONS

7.1 Blockchain Technology

[207] Blockchain technology utilises two core technologies to create a persistent, tamper-evident record of transactions between parties whose identity has been authenticated.⁵⁰⁴ First, hash pointers link blocks of transactions together, such that tampering with transaction data in past blocks breaks the links between the blocks.⁵⁰⁵ Second, Public Key Infrastructure establishes parties’ identities, with private keys used to encrypt data and provide digital signatures.⁵⁰⁶

⁵⁰⁰ See NISTIR OVERVIEW, *supra* note 6, at 33.

⁵⁰¹ See *id.* at 41–42.

⁵⁰² See discussion *supra* Section 3.3.2., at [71].

⁵⁰³ See Buterin, *Public and Private Blockchain*, *supra* note 138.

⁵⁰⁴ See generally discussion *supra* Section 2 (discussing data integrity and identity authentication).

⁵⁰⁵ See discussion *supra* Section 2.1.2, at [16]–[17].

⁵⁰⁶ See discussion *supra* Section 2.2, at [21]–[23].

[208] Blockchain technology can be deployed in various ways to create platforms with different features, including with regard to:

- (i) Access: who can propose new transactions to be added to the ledger;
- (ii) Control:
 - a. storage: who stores a copy of the ledger;
 - b. mining and consensus: how to create new blocks and determine when blocks should be added to the existing ledger;
 - c. governance: who controls the platform's underlying software;
- (iii) Visibility: who can view the ledger;
- (iv) Identity: whether users are identifiable; and,
- (v) Automation: whether the platform supports smart contracts.

[209] Early cryptocurrencies were set up with the following features: an open, distributed platform (where anybody can store a copy of the ledger as a node, and contribute to the process of adding new blocks as a miner); open/permissionless access (where anybody can join as a user); and, a public database (where anybody can view the transaction records stored on the blockchain or store a copy of the ledger).⁵⁰⁷ In order to ensure the consistency of the many distributed copies and to ward off attackers, these systems rely on resource-intensive consensus protocols.⁵⁰⁸ They offer strong data integrity, since it is much harder to tamper with large numbers of distributed copies, as well as high resilience.⁵⁰⁹ However, the need to support thousands of small nodes, and run proof of work, limits transaction throughput and increases costs.

⁵⁰⁷ See discussion *supra* Section 3, at [32].

⁵⁰⁸ See discussion *supra* Section 3.1.4.

⁵⁰⁹ See discussion *supra* Section 3.1.4.

[210] These systems also provide a high level of transparency, since anyone can view all transaction data.⁵¹⁰ To afford users some level of privacy, the systems are pseudonymous: users are identified only by their public key and an address, which does not directly reveal a real-world identity.⁵¹¹

[211] By contrast, future applications of blockchain will include more centralised platforms, with closed/permissioned use, and a private database. In such arrangements, a TTP or group of trusted nodes store copies of the ledger, add new blocks, and determine which users can access the platform and view the ledger.⁵¹² This requires users to have a level of trust in the centralised blockchain administrator(s) to maintain an accurate ledger and keep the ledger secure and the system running.⁵¹³ Since there are only a limited number of trusted nodes, such systems do not need resource-intensive consensus protocols. Further, by working with a small number of high-capacity nodes, the systems may be better able to scale and process large numbers of transactions.

[212] In sum, from a technical perspective, whether to use an open, distributed or more centralised approach will depend on the degree of trust needed and the application's requirements for data integrity, resilience, scalability, and confidentiality.⁵¹⁴ It is not clear that using a centralised blockchain offers significant advantages over existing database solutions,

⁵¹⁰ See Buterin, *Public and Private Blockchain*, *supra* note 138.

⁵¹¹ See discussion *supra* Section 4.2.

⁵¹² See discussion *supra* Section 3, at [51]–[54].

⁵¹³ See discussion *supra* Section 3, at [28].

⁵¹⁴ Cf. Gideon Greenspan, *Blockchains vs Centralized Databases*, MULTICHAIN (Mar. 17, 2016), <https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/> [<https://perma.cc/HA5A-5798>] (comparing various aspects of blockchains and centralized databases to show that choosing between the two “comes down to a series of trade-offs”).

particularly when traditional databases can perform many of the same functions.⁵¹⁵

7.2 Blockchain and the Law

[213] Given the diversity of possible blockchain platform designs, no *one-size-fits all* legal analysis is possible. Instead, each application of blockchain technology will need to be considered on its facts. From a legal perspective, closed, centralised platforms are generally likely to entail lower risks in the areas we have reviewed. The TTP or group of trusted nodes may be able to coordinate compliance, limit visibility of records, and reverse past transactions if necessary. Achieving these goals is harder on open, distributed platforms that deliberately lack a central administrator with control over the ledger.

[214] To illustrate this point, we reviewed issues that may arise in various areas of the law. For example, users on blockchain platforms engage in activities, such as setting up smart contracts and issuing ICOs, that have characteristics closely resembling established legal concepts, such as contracts and securities. Engaging in these activities may have significant legal consequences. In many cases, the legal implications are affected by the blockchain platform's design, as set out below.

7.2.1 Contract Law

[215] The legal concept of *contract* is generally not subject to formal requirements. As a result, communications relating to smart contracts may qualify as enforceable legal contracts, giving rise to legal obligations that go beyond the underlying computer code. Smart contracts may entail particularly high risks, since they combine automatically executed code

⁵¹⁵ See e.g. Arvind Narayanan, '*Private Blockchain*' Is Just a Confusing Name for a Shared Database, FREEDOM TO TINKER (Feb. 18, 2014), <https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/e> [https://perma.cc/A5MV-ZSSK].

written by fallible humans with a blockchain's persistent, tamper-evident data structure. For example, a bug in the smart contract's code may lead to non-performance, or incorrect performance of a legal contract. The ease of correcting such mistakes will depend on the type of blockchain platform involved. Centralised blockchain platforms can support reversibility better: the TTP or group of trusted nodes may be able to correct any mistakes by amending erroneous transactions in the ledger, since they control the copies. However, on an open, distributed platform, correcting past mistakes would be more difficult, potentially requiring cooperation from thousands of nodes.

7.2.2 Data Protection Law

[216] If a blockchain platform is used to process personal data, the users, nodes, and miners of blockchain platforms may be either data controllers, processors, or potentially both. If so, they will need to comply with data protection obligations and may be exposed to substantial penalties for breaches of data protection laws. With open, distributed platforms, even if all parties involved were deemed joint controllers, it is not clear how they would comply with their obligations (such as to establish responsibilities by contract and respond appropriately to the exercise of data subjects' rights).

7.2.3 Securities and Property Law

[217] Depending on their function, the tokens sold in some ICOs may be deemed to be securities, in which case their promoters will need to comply with securities laws, including obligations to provide investors with appropriate information. Whether the tokens issued under ICOs qualify as the legal *property* of their users is currently uncertain and will likely depend, to some extent, on the rights the token purchaser holds against the issuer. In England and Wales, a transferable token that gives the user a definable right against a specific issuer may qualify as a chose in action. Conversely, the property status of cryptocurrency tokens on open, distributed applications like Bitcoin is unclear.

7.2.4 Intellectual Property Law

[218] Some blockchain databases may qualify for a *sui generis* database protection right. If so, the right holder would have the right to prevent extraction and re-utilization of the contents of that database. Determining the *maker* of the database (who is awarded the right) could be fairly straightforward for centralised platforms, but may be more challenging with open, distributed platforms.

7.2.5 Company Law

[219] Finally, establishing a company is generally subject to formal requirements, such as registration with a central agency. As a result, DAOs are unlikely to qualify as legal persons and, as a result, participants will not necessarily benefit from limited liability. As with smart contracts, DAOs combine human fallible code with a blockchain's persistent database. Should a bug in the code lead to liability for damages, each DAO participant could conceivably be liable. As noted above, any such damages would be much more difficult to reverse in the case of open, distributed platforms.

[220] Ultimately, the legal uncertainties and risks associated with the use of open, distributed platforms may limit their adoption. In some cases, technical solutions may be available, or be developed, to provide greater certainty and reduce such risks. In other cases, legislators, regulators, and legal advisers may need to design novel legal solutions.