THE MODERN LAW REVIEW

The Governance of Blockchain Financial Networks

Philipp Paech*

Since the emergence of the virtual currency Bitcoin in 2009, a new, Internet-based way of recording entitlements and enforcing rights has increasingly captured the interest of businesses and governments. The technology is commonly called 'blockchain' and is often associated with a closely related phenomenon, the 'smart contract'. The market is now exploring ways of using these concepts for financial assets, such as securities, fiat money and derivative contracts. This article develops a conceptual framework for the governance of blockchain-based networks in financial markets. It constructs a vision of how financial regulation and private law should set the boundaries of this new technology in order to protect market participants and societies at large, while at the same time allowing the necessary room for innovation.

INTRODUCTION

In this article, I will explore the regulatory and private law issues arising from the use of blockchain networks in financial markets, including relevant issues pertaining to the control of such networks and to the influence of the market on their development. I refer to the entirety of these aspects as 'governance', intentionally adopting a broad understanding of this term.[1] The analysis establishes whether and to what extent blockchain-based business models can exist outside the regulatory and supervisory perimeter that generally applies to financial institutions. It further investigates the role of private law within these networks, notably in ensuring the smooth functioning of risk-based regulation and in avoiding a risk-shift towards non-adjusting third parties. Lastly, the article assesses the need for cross-jurisdictional co-ordination. It is conceived as a mapping exercise, constructing a vision of the core governance issues and their interdependencies, thus providing the conceptual foundation for a future governance framework.

The emergence of blockchain technology has become inextricably linked to Bitcoin,[2] a 'virtual currency' that allows users to trade 'bitcoins' directly from peer to peer without involving banks or other intermediaries.[3] Whereas

*Assistant Professor of Law, London School of Economics and Political Science. I am grateful to Jan Kleinheisterkamp, Klaus Löber, Eva Micheler, Sarah Paterson and the two anonymous reviewers for their comments on earlier drafts, to Martin Walker for inspiring discussions and to Katerina Papapanagiotou for research assistance.

1 See M. Bevir, *Key Concepts in Governance* (London; Thousand Oaks CA: Sage, 2009) 29-30.
2 G. W. Peters and E. Panayi, 'Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money' Working Paper, 18 November 2015 at https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2692487, 3 (unless otherwise stated, all URLs were last accessed 30 November 2016).
3 The paper that laid the foundations for Bitcoin and the blockchain technology is S. Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' Working Paper, 2009 at

 (2017) 80(6) MLR 1073–1110

Published by John Wiley & Sons Ltd, 9600 Garsington Road, Oxford OX4 2DQ, UK and 350 Main Street, Malden, MA 02148, USA

Bitcoin in theory is nothing more than a unit of account, it has in practice developed functions akin to those of money, in particular since it can be freely exchanged against currency and is regularly used to store value.[4] Bitcoin has also risen to prominence as a means of payment (over 100,000 retailers accept bitcoins)[5] and as a means of speculation[6] beyond the circles of Internet aficionados in the space of just a few years. It has also gained notoriety as being susceptible to speculative bubbles, and as the object of criminal activity.[7] Given these characteristics, virtual currencies have 'a good claim of being regarded as money'.[8] However, legal categorisation is unclear and a new legal category might be needed to recognise 'virtual *choses* in possession' as a new form of property.[9]

The easiest way to understand what blockchain technology stands for is to think of it as an Internet-based database to store entitlements, of which identical copies of equal constitutive value are held by every network participant. The database enables each participant to trade these entitlements by instructing the database software accordingly, which will then autonomously and irreversibly effect the relevant changes to the network participants' holdings (in addition to 'database', the terms 'ledger' and 'record' are also used). This was the idea originally introduced with the Bitcoin network. Later on, blockchain networks emerged that were more flexible in terms of what could be recorded in the database, the most important of these probably being the Ethereum network, which also allows users to trade entitlements but which can, in addition, record and autonomously run self-executable programmes, the so-called 'smart contracts'.[10]

Meanwhile, the technology has been extended further to take in 'real' things,[11] and may soon be used for a wide range of financial assets, ie those

https://bitcoin.org/bitcoin.pdf; for a comprehensive description, see, Peters and Panayi, *ibid*, 2-9; for a technical but still accessible description, see E. Wall and G. Malm, 'Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository' Masters thesis, Lund University 2016 at http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8885750&fileOId=8885765.

4 See C. Procter, *Mann on the Legal Aspect of Money* (Oxford: OUP, 7th ed, 2012) 1.170-1.172.

5 A. Cuthbertson, 'Bitcoins now accepted by 100.000 retailers worldwide' *International Business Times* 4 February 2015 at http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613. See also, www.coindesk.com/information/what-can-you-buy-with-bitcoins/.

6 See N. Mancini, 'Bitcoin: Rischi e Difficoltà Normative' (2016) 35 *Banca Impresa Società* 131; I. Kaminska, 'The *Mt. Gox* Bitcoin Bubble' *Financial Times* 4 August 2016 at https://ftalphaville.ft.com/2015/08/04/2136420/the-mt-gox-bitcoin-bubble/.

7 See Kaminska, *ibid*; K. Scannell, 'Founder of Silk Road given Life in Prison' *Financial Times* 29 May 2015 at www.ft.com/content/8694f87c-0646-11e5-89c1-00144feabdc0.

8 Financial Markets Law Committee, 'Issues of legal uncertainty arising in the context of virtual currencies' 2016 at http://www.fmlc.org/uploads/2/6/5/8/26584807/virtual_currencies.pdf, 23 (last accessed 7 May 2017).

9 *ibid*.

10 See https://ethereum.org; K. Werbach, 'Trustless Trust' Working Paper, August 2016 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844409.

11 For instance diamonds (http://www.everledger.io), government services in Estonia ranging from healthcare to electronic court procedures (https//e-estonia.com/component), crowd-funding applications (see A. Sunnarborg, 'Blockchain Startups Make Up 20% of Largest Crowdfunding Projects' *Venturebeat* 15 May 2016 at http://venturebeat.com/2016/05/15/

assets that, unlike virtual currencies, represent a claim against another party. With such technology, shares or bonds could be issued,[12] traded and settled on the blockchain networks, thereby replacing stock exchanges, clearing houses and settlement systems.[13] Indeed, the technology could be used to make all kinds of payment,[14] and central banks could issue fiat money in this way.[15] Likewise, derivative contracts could be concluded, administered and settled within blockchain networks.[16] In this article, I refer to these and similar emerging structures (to the exclusion of virtual currencies) as 'blockchain financial networks'.

The financial industry has already spent over 1.4bn USD on research into blockchain[17] as it is expecting immense benefits from moving to the new technology; banks are hoping to save 15–20bn USD on their infrastructure by 2022.[18] At the same time, Fintech businesses are preparing to enter the financial market with innovative blockchain-based services,[19] while regulators and legislators are considering how to accommodate the new technology.[20] Yet

blockchain-startups-make-up-20-of-largest-crowdfunding-projects/), and music royalties (G. Howard, 'Bitcoin for Rock stars – A Year Later' *Forbes* 25 September 2015 at http://www.forbes.com/sites/georgehoward/2015/09/25/bitcoin-for-rock-stars-a-year-later-an-update-from-d-a-wallach-on-blockchain-and-the-arts-part-1/#cd82c6522493).

12 See G. Chavez-Dreyfuss, 'Overstock to Issue Stock to be traded on Blockchain Platform' *Reuters* 16 March 2016 at www.reuters.com/article/us-overstock-bitcoin-stocks-idUSKCN0WI2YA; Nasdaq, 'Nasdaq Linq enables first-ever private securities issuance documented with blockchain technology' Press release, 30 December 2015 at http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326.

13 See DTCC, 'Embracing Disruption—Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape' January 2016 at www.dtcc.com/news/2016/january/25/blockchain-white-paper; Euroclear and Slaughter and May, 'Blockchain Settlement—Regulation, Innovation and Application' November 2016 at www.euroclear.com/en/campaigns/Blockchain-settlement-Regulation-innovation-and-application.html; Euroclear and Oliver Wyman, 'Blockchain in Capital Markets' February 2010 at www.euroclear.com/en/campaigns/blockchain-in-capital-markets.html.

14 See, for example, Ripple, 'Settlement of international wholesale payments' at https://ripple.com; Circle (consumer payment services in EUR, USD, GBP) at www.circle.com/en-gb.

15 See B. Broadbent, Deputy Governor of the Bank of England, 'Central Banks and Digital Currencies' Speech at London School of Economics and Political Science, 2 March 2016 at www.bankofengland.co.uk/publications/Pages/speeches/2016/886.aspx; J. Wild, 'Central banks explore blockchain to create digital money' *Financial Times* 2 November 2016 at www.ft.com/content/f15d3ab6-750d-11e6-bf48-b372cdb1043a; A. Sharp, 'Bank of Canada to publish payment experiment result in coming months' *Reuters* 20 November 2016 at www.reuters.com/article/canada-cenbank-blockchain-idUSL1N1D31J5?feedType=RSS&feedName=bondsNews.

16 See L. Brain, 'Barclay's Smart Contract Templates' video, London, 18 April 2016 at https://www.r3cev.com/projects/; A. Karphal, 'Barclay's used blockchain technology to trade derivatives' CNBC 19 April 2016 at www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-trade-derivatives.html.

17 See World Economic Forum, 'The future of Financial Infrastructure' August 2016 at https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services/, 14.

18 See Santander, 'Fintech 2.0—Rebooting Financial Services' June 2016 at https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf.

19 See, for examples, n 13 above and Clearmatics (securities and derivatives settlement) at http://www.clearmatics.com; Epiphyte (foreign exchange settlement) at http://epiphyte.com.

20 See European Parliament, Resolution of 26 May 2016 on Virtual Currencies, Doc No P8_TA(2016)0228); Financial Conduct Authority (UK), 'Financial Conduct Authority

however great the current interest in blockchain technology, its adoption is still in its early infancy and very much in flux. Potential applications range from the original, highly disruptive concept underlying Bitcoin or Ethereum, which involves open, largely anonymous, unregulated peer-to-peer networks that eliminate the need for financial intermediaries, to rather unspectacular projects that use only certain parts of the blockchain technology, notably the distributed database, to modernise and harmonise IT infrastructure in a quest for greater efficiency without attempting to overthrow existing market structures.[21]

The disruptive potential of blockchain technology applies not only to existing business models but also threatens the effectiveness of the existing governance framework for financial markets, depending on how the technology is deployed. It is important, therefore, to set the axioms of a governance framework for blockchain financial networks at an early stage in order to further a potentially beneficial market development and avoid the cost of adjusting market practice to new rules at a later stage.[22]

My starting point in the second part of this article will be an analysis of the three ground-breaking characteristics of blockchain networks (ie, distributed ledgers, the immutability of the acquisition process and the record, and the possible storage of auto-executable smart contracts in a blockchain database) that could effect structural changes in market practice and may render traditional governance concepts ineffective.

The third part of this article contemplates the characteristics of blockchain technology in the light of existing financial regulation. Originally, blockchain technology was conceived for state-remote networks, ie networks entirely self-governed on the basis of consensus amongst their users. Nevertheless, blockchain financial networks may create risks that might have an impact on the wider market, notably by transmitting systemic risk, discriminating between market actors and facilitating illegal activity. Hence, blockchain financial networks cannot remain outside the regulatory perimeter.

The fourth part of this article looks at private law and the treatment of individual rights in blockchain financial networks. Here, crucially, software may be seen as the sole determinant for enforceability, thus bypassing the relevant rules of private law and the authority of the courts. Such a strict technology-based solution for balancing diverging interests may be acceptable if confined to the actual parties to a blockchain-based transaction as an expression of their contractual freedom. However, since third parties and the market at large may also be affected, the issue of enforceability of rights cannot be left entirely to the software, even if the parties themselves agree to transact following the internal rules of the network.

The fifth part of the article discusses two factors that are instrumental in shaping regulatory and legislative strategies appropriate for a range of future

unveils successful sandbox firms on the second anniversary of Project Innovate' Press release, 7 November 2016 at www.fca.org.uk/news/press-releases/financial-conduct-authority-unveils-successful-sandbox-firms-second-anniversary.

21 See n 13 above.

22 See A. Wright and P. De Filippi, 'Decentralized Blockchain Technology and the Rise of *Lex Cryptographia*' Working Paper, 12 March 2015 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, 56.

applications of blockchain technology to financial transactions. The first such factor is the extent to which regulated financial institutions are involved in blockchain networks; if they are, much of the existing regulation can be applied. An equally important issue is the international reach of blockchain financial networks, which may render domestic governance frameworks largely ineffective, unless there is appropriate international co-ordination.

The final part of the article sets out my conclusions.

A NEW MARKET PRACTICE AND THE TRADITIONAL LINCHPINS OF GOVERNANCE

Blockchain came to be counted among the 'disruptive' technologies very early on, ie, it was spotted as one of those typically Internet-based platforms that have the potential of unravelling traditional market structures, as has happened in other areas such as transport by taxi (Uber), holiday accommodation (Airbnb) and telecommunications (WhatsApp). Typically, disruptive technologies may modify the value chain of a traditional business, thereby threatening the incumbents' income models.

Blockchain technology enables disrupters and incumbents to reconceptualise business models in financial markets. As a result, existing ways of trading and administering financial assets might change considerably were blockchain technology to be adopted on a wider scale. However, the resulting changes will affect a number of aspects that today serve as linchpins linking regulation and private law to market practice. These elements are deeply anchored in our understanding of how financial markets work and how we govern them. If they disappear or change, governance strategies will need to be adapted accordingly.

Three characteristics of blockchain technology have the potential of turning our understanding of how the market functions upside down, and may affect the current governance framework accordingly, as we will see later in the third and the fourth parts of this article. First, the concept of the distributed ledger that lies at the heart of blockchain affects the central role of intermediation and client accounts or, more broadly, intermediary-client relationships; secondly, failproof, automated acquisition processes and immutable records replace trust in intermediaries and create a new form of truth; and lastly, blockchain technology renders the execution of smart contracts truly unstoppable, which means that, in the absence of built-in circuit breakers, all human discretion is excised from the execution and enforcement of contractual duties.

Distributed databases, disintermediation and the disappearance of client accounts

Financial transactions, such as the payment of money, the sale and purchase of securities, the exchange of currencies or derivative contracts, in principle represent a bilateral relationship between the relevant parties. However, they are typically concluded, administered or settled using intermediaries such as banks or brokers, and financial market infrastructures such as stock exchanges, payment systems, securities settlement systems or derivatives central counterparties. Intermediaries and infrastructures form networks that link financial market actors with one another. These networks are traditionally ordered either in a centralised or a decentralised fashion.

Centralised networks rely on a single record in which all transactions and holdings are recorded by a trusted central entity; only in this way can market participants reach consensus on relevant facts, in particular their holdings.[23] In several countries, for instance, a central securities depository maintains securities accounts for all market participants that invest in securities. All acquisitions and dispositions are recorded in that register, and each individual balance is retrievable there.[24] *Decentralised* networks, on the other hand, are characterised by a structure in which different records *together* provide complete information on transactions and holdings. No single record on its own holds that comprehensive information. For instance, in some jurisdictions the central securities depository records the transactions and holdings of banks and brokers but not of end-investors. The assumption is that these banks and brokers will record the identity of investors to whom the securities ultimately belong in their own ledgers.[25]

Different as they may be, the centralised and decentralised financial network models do share an important feature: the original two-party relationship between the parties to a transaction (seller-buyer) is replaced by several two-party relationships between the parties and their intermediary and, as the case might be, between additional intermediaries providing the necessary links in the network.[26] The technical process of recording an entitlement to an asset takes place on the IT system of the relevant intermediary. This record is associated with the legal relationship between the intermediary and its client, generally called an account or, more broadly, the client relationship. In modern financial markets, this account or client relationship is one of the linchpins of financial regulation and private law: property rights are defined by and contractual duties arise from it, as do a plethora of behavioural rules set by financial regulation.

By contrast, blockchain technology is based on the idea of a *distributed* record. Here, each participant in the network ('node'), in practice a computer server controlled by a market participant and fitted with the relevant blockchain platform software, maintains a complete record of past transactions. All nodes are constantly updated with information on the latest transactions. As a consequence, all transaction information is available at any node at any given point in time, is identical and has equal constitutive value, ie there are no master and subordinated records.[27] Thus, blockchain introduces an organising principle into the financial markets that is not built on a two-party relationship between

23 *ibid*, 5.
24 See Unidroit, 'Working Paper regarding so-called Transparent Systems' 2006 Unidroit S78-44 at http://www.unidroit.org/english/documents/2006/study78/s-78-044-e.pdf.
25 See P. Paech, 'Securities, Intermediation and the Blockchain—An Inevitable Choice between Liquidity and Legal Certainty' (2016) 21 *Uniform Law Review* 8.
26 *ibid*, 15-16.
27 Nakamoto, n 3 above, section 5; P. De Filippi and B. Loveluck, 'The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure' (2016) 5 *Internet Policy*

investors and intermediaries and between intermediaries and infrastructures.[28] There are no intermediaries, hence no accounts or other intermediary-client relationships within the blockchain network, so that an important linchpin of financial regulation and private law concepts is missing *within* the network itself.

However, intermediation may still occur *outside* the network. Nodes may have clients which are not part of the network. In such a scenario they may transact on the network in their own name but on behalf of these clients, ie operate as intermediaries for persons outside the network.[29]

Considering the 'disintermediation' within the network itself it becomes clear that there is enormous potential to change the market. In order to understand it we must consider the current ecosystem of financial holdings and transactions. Financial intermediaries and infrastructures are only rarely involved in moving tangible assets around. Banks hold book-money in electronic accounts and transfer it through electronic payment systems. Similarly, shares, bonds and derivatives are typically incorporeal and purely account-based. In fact, the lion's share of the services provided by the financial service industry relates to data storage and data processing.

However, the relevant IT systems they use differ considerably: as between different types of asset, different types of service provided in relation to an asset, different jurisdictions and even as between individual financial institutions. The same asset is typically mirrored repeatedly in different systems maintained by different entities, potentially in different jurisdictions. This historically generated multiplication and diversification of records and account relationships leaves ample room for inefficiencies and operational and legal risk:[30] the constant reconciliation of these records is costly and slow; there are frequent temporary mismatches; investors are increasingly disconnected from issuers because the relevant investor rights are degraded down to the smallest feature common to all accounts used to hold a specific security;[31] extracting aggregate data, for example for supervisory purposes, is a cumbersome exercise that often results in unsatisfactory results;[32] as a given asset appears in different independent records it may be unclear which record is constitutive and which is only for book-keeping purposes; or, for the same reason, an asset may be used simultaneously by different parties, eg, it might be pledged by different market participants for their own purposes, simply because the same asset appears in various accounts.[33]

In the case of distributed records used in blockchain networks, all parties involved in holding and administering an asset have an up-to date copy of

Review 7 at https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure.

28 Wright and De Filippi, n 22 above, 2.

29 See below 1102.

30 Paech, n 25 above, 15-22.

31 See E. Micheler, 'Custody Chains and Asset Values: why crypto-securities are worth contemplating' (2015) 74 *Cambridge Law Journal* 509.

32 See Euroclear and Oliver Wyman, n 13 above, 7.

33 See Peters and Panayi, n 2 above, 22-23 for an overview of the various ledgers held within a financial institution for accounting and regulatory purposes.

the same record at their disposal at all times, a record that is so designed as to exclude mismatches with the other copies.[34] In addition, blockchain technology allows for greater data depth. That is, records are able to store more complex information than accounts typically can today.[35] For instance, a traditional securities account with a broker records ownership of securities but nothing else. More in-depth information in relation to these securities needs to be generated and held in separate records. In a future blockchain-based setting, information as to ownership of a specific share could extend to information as to which service providers are involved in its administration, whether the share is encumbered and if so, in whose favour. In addition, self-executing programmes, so-called 'smart contracts' (which I will discuss below), can be recorded together with the ownership information and could, for instance, automatically process dividend or interest payments once they are due.

In other words, the industry could move from a multitude of records relating to the same asset and maintained for different purposes, and which are not properly co-ordinated, to a single record[36] distributed amongst and used by all parties, or at least significantly reduce the number of different records. Because the blockchain record is distributed amongst all nodes, the relevant financial institutions and infrastructures are able to provide their services in relation to a specific asset on the basis of the same information. Significant parts of the financial industry, including most 'global players', have identified these benefits as their common interest and have formed consortia supporting technology start-ups, such as the R3CEV and Hyperledger, that are currently developing the relevant blockchain software.[37]

As a consequence, the considerable operational complications caused by multiple records could be removed in the future, as would be the associated uncertainty and cost. The speed of settling transactions would increase.[38] At the same time, reporting to the competent supervisor would be facilitated, as the relevant data could be made available by giving the supervisor access to the blockchain record.[39]

A fail-proof system, the displacement of trust and the redefinition of truth

A distributed record as described above is only the base component of a blockchain network. In particular, additional mechanisms are needed to guarantee that the updates of records kept by nodes reflect the truth, since practically any node would be in a position to propose updates to the other nodes, including fraudulent ones.

34 See Nakamoto, n 3 above, 3-4; Wall and Malm, n 3 above, 8-16.
35 P. Ortolani, 'Self-enforcing Online Dispute Resolution: Lessons from Bitcoin' (2016) 36 *Oxford Journal of Legal Studies* 595, 608.
36 Peters and Panayi, n 2 above, 24.
37 https://www.r3cev.com and https://www.hyperledger.org.
38 Peters and Panayi, n 2 above, 17, 27.
39 *ibid*, 18.

Traditionally, the truthfulness of records in financial markets is ensured through a mechanism involving trust (in the everyday sense of the word[40]) and responsibility. Clients trust their intermediaries to keep records diligently so that they reflect the true state of holdings at any given time. Reputation may be the original bedrock of this trust, but more importantly today it is a question of regulation: clients typically trust financial institutions because they know they are authorised and supervised.[41] Clients expect intermediaries to be able to correct erroneous records, and to do so either voluntarily or compelled by the judiciary.[42] In other words, regardless of the outcome of the technical process of record keeping, intermediaries and, ultimately, the courts have the last word as to whether rights such as securities or cash in accounts have been acquired or lost and, hence, whether the relevant record entries correspond to the truth.

By contrast, the inventors of blockchain relinquished the current model for ensuring truthful outcomes built on *ex-ante* regulation-induced trust and *ex-post* review by the courts.[43] Instead, blockchain technology relies entirely on a technology-based solution giving nodes the certainty that transactions are correctly executed and accurately recorded. In addition to the idea of a distributed record (see preceding section), the concept builds, first, on a process to establish consensus amongst nodes regarding the correctness of an update of a record on the basis of a mathematical-probabilistic approach (this process is called the 'proof of work' in the *Bitcoin* context) and, secondly, on a process by which all processed transactions are locked in a chain of sequential, logically intertwined sets, or 'blocks', that cannot be changed – in principle[44] – once a new block of transactions has been validated by the nodes (this latter feature is the origin of the term 'blockchain').[45]

For such a system to work, however, it is imperative that no person or group be in a position to take control of the majority of nodes and thus of the validating process. This goal is achieved by conceiving the network as 'permission-less',[46] ie, as an open network. Anyone with the necessary (freely available) hardware and software can join *Bitcoin*, *Etherium* and other networks as a node following this strict logic. Even though this openness may allow fraudsters to join, the idea is that the well-nigh unlimited reservoir of computing power spread across the globe can theoretically be made available to the network and will always be greater than the computing power of a potential attacker, thus rendering the network tamper-proof and censorship-resistant.[47] Newer blockchain networks, in particular those set up amongst financial institutions, depart from this logic and restrict access to their networks, for instance to members in a specific

40 Though this 'is one of those "I know it when I see it"', Werbach, n 10 above, 8. See, for a discussion of 'trust', *ibid*, 8-15.
41 *ibid*, 15-16.
42 Ortolani, n 35 above, 607.
43 Nakamoto, n 3 above, 1; M. Raskin, 'The Law of Smart Contracts' Working Paper, 22 September 2016 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2842258, 7.
44 See text to notes 66-67 and 84 below.
45 See Nakamoto, n 3 above, 1-4; Wall and Malm, n 3 above, 5-23.
46 Nakamoto, *ibid*, 8.
47 Nakamoto, *ibid*, 3; Wall and Malm, n 3 above, 7. For a critical assessment, see, De Filippi and Loveluck, n 27 above, 14-17.

consortium.[48] However, this is possible only because these networks imply some level of trust amongst nodes.[49] Hence, the 'permissioned' model of blockchain networks is different not only in that it requires permission to access. In actual fact, these networks are based on fundamental assumptions different from those of the original blockchain technology.[50]

Smart contracts and unstoppable execution

The term 'smart contract' refers to computer code that is designed automatically to execute contractual duties upon the occurrence of a trigger event.[51] The simple example of a vending machine has been cited to explain the concept: upon insertion of a specific type of coin, the computer programme instructs the mechanism of the machine to release the good.[52] This concept was not originally part of the blockchain idea. It might be described as an add-on extending the capabilities of the blockchain network beyond its function as a keeper of records.

A smart contract 'excises human discretion from contract execution'.[53] Unlike the performance of contracts generally, performance on a smart contract cannot be stopped, neither voluntarily by the parties (ie it can neither be breached nor amended), nor by a central entity, nor by a court or supervisor.[54] Accordingly, the idea of smart contracts is different from that of the automated or high-speed execution of contracts, as the certainty of performance is the core issue here but not its speed or reduced cost of labour.

The absolute certainty of performance makes contracting much more efficient as the counterparty risk and settlement risk typically inherent in contracts are considerably reduced, if not eliminated. A simple example is the securities collateral kept in a blockchain network: if the debtor has not paid by a certain date, the smart contract autonomously transfers the securities to the creditor. Furthermore, the precision of the programming language is much greater than that of written human language; in particular, warranties and conditions can be formulated with much greater accuracy,[55] and contracts can be treated and processed in data formats.[56] Hence, it is argued, smart contracts make transacting considerably less expensive owing to certainty of execution and the near-zero risk of litigation in court.[57]

48 Peters and Panayi, n 2 above, 6.
49 *ibid*.
50 *ibid*, 7.
51 H. Surden, 'Computable Contracts' (2012) 46 UC Davis L Rev 629, 656-657; Ortolani, n 35 above, 608; Raskin, n 43 above, 2; J. Stark, 'Making Sense of Blockchain Smart Contracts' *Coindesk* 4 June 2016 at http://www.coindesk.com/making-sense-smart-contracts/; Wright and De Filippi, n 22 above, 11. N. Szabo, 'Formalizing and Securing Relationships on Public Networks' (1997) 2 *First Monday* at http://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First (last accessed 15 November 1997).
52 Szabo, *ibid*.
53 Raskin, n 43 above, 2.
54 Wright and De Filippi, n 22 above, 25-26.
55 Raskin, n 43 above, 21-22.
56 Surden, n 51 above, 690-694.
57 See Raskin, n 43 above, 33; Surden, *ibid*, 689.

In the financial markets, smart contracts could be used for a variety of functions. For instance, a bond held in a blockchain network might have a smart contract attached to it that automatically executes interest payments on the payment date, and the amount to be paid is determined on the basis of data retrieved from a predefined, reliable Internet source. A second example relates to the derivatives market.[58] Parties might enter derivative contracts electronically; the relevant building blocks of that short programme would automatically be taken and assembled from an electronic contract library set up to this effect. The smart contract could be so designed as to automatically cater for due payments to be executed and to adjust collateral levels between the parties. Also, upon termination of the contract, the programme could autonomously calculate the due termination amount to be paid. Again, amounts would depend on reference data sourced from a predefined, reliable data provider.

Interestingly, the (older) concept of smart contracts will achieve its full potential only if combined with the (newer) invention of blockchain networks.[59] This is because the certainty of execution is not absolute as long as human discretion can interfere with the process: the vending machine is technically still under the control of its owner. In the context of financial markets, the issue is that IT systems, for example those running cash and securities accounts, are still controlled by a financial intermediary who can alter the process, either voluntarily or in compliance with a court or supervisory order. By contrast, the record of a blockchain network on which a smart contract is stored is supposed to be absolutely immutable and its execution automatic. As set out in the previous section, autonomy of execution is a direct consequence of the fact that blockchain networks operate without any central or trusted entity to balance the parties' interests.[60] In other words, it is only in blockchain networks that there is truly no *ex post* review of contractual duties after contract formation.[61] The only way to influence the execution of smart contracts is by programming them in such a way that they seek external input on the further execution (from a non-smart, human-controlled IT process into which they are embedded, or from an authority or court) at the occurrence of certain, predefined events.[62] This is the point in time at which further execution can be aborted or otherwise influenced, yet exclusively on the basis of pre-programmed options.

Smart contracts can theoretically be combined and thus interact with one another in a decentralised and distributed structure, operating autonomously, ie without human intervention, once deployed by their programmers on the basis of the rules and mechanisms programmed into them.[63] Such 'decentralised autonomous organisations' (DAOs) could even enter into new smart contracts with other market actors, creating a complex, evolving ecosystem of interacting agents linked by pre-determined, hard-wired and self-enforcing rules.[64] They

58 See Brain, n 16 above.
59 Werbach, n 10 above, 30.
60 Ortolani, n 35 above, 607.
61 See Raskin, n 43 above, 7, 14.
62 *ibid*, 24. See also text at notes 143-145 below.
63 Wright and De Filippi, n 22 above, 15; Surden, n 51 above, 694-695.
64 Stark, n 51 above; Wright and De Filippi, *ibid*, 17.

are not owned or controlled by any single person or corporation; yet they can interact with the market.[65]

The most important DAO so far was created on the basis of smart contracts recorded and processed on the Ethereum network:

> A humanless venture capital firm that would allow the investors to make all the decisions through smart contracts. There would be no leaders, no authorities. Only rules coded by humans, and executed by computer protocols.[66]

It raised a spectacular 150m USD of which 50m were subsequently diverted by a malicious node to a private Internet address, leading to the project being abandoned.[67] Still, similar projects may emerge in the future despite this failure. By contrast, it is not yet clear whether and to what extent the financial industry will develop an interest in such *entirely* autonomous, self-referential actors since, as for-profit organisations, they ultimately need to keep legal and economic ties with the device and exercise some control over it. In any case, the somewhat extreme concept of totally autonomous self-executing software shows that smart contracts stored on a blockchain network can operate in varying degrees of autonomy from humans and on a smaller or larger scale, providing input to one another in the form of reference data and triggering events, potentially across different blockchain networks. Obviously, the more intertwined smart contracts become and the lower the degree of control by humans, the more difficult it will be to govern this phenomenon.

BLOCKCHAIN FINANCIAL NETWORKS AND STATE REGULATION

The inventors of blockchain technology aimed at creating self-governing and state-remote networks, as epitomised by *Bitcoin*. Nobody should be able to interfere in the governance of the network from outside the circle of its nodes: in particular, states should be unable to censor or regulate it. Instead, internal processes are deemed to balance all the relevant interests so that no judicial or regulatory intervention is needed.[68] Nevertheless, since blockchain-based virtual currencies provide individuals with a means of payment and an easy and near-anonymous method of transferring value, states are considering relevant regulation, mainly targeting money laundering and terrorist financing.[69] Beyond this very specific rationale, the role of blockchain financial networks in which

65 Wright and De Filippi, *ibid*, 54.
66 J. I. Wong and I. Karr, 'Everything you need to know about the Ethereum "Hard Fork"' *Quartz* 18 July 2016 at http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/.
67 See Wong and Karr, *ibid*.
68 De Filippi and Loveluck, n 27 above, 3-4.
69 See European Parliament, n 21 above; EU Commission, 'Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 [etc]' 5 July 2016, COM(2016) 450 final; New York Codes, Rules and Regulations, Title 23 Chapter I Part 200 – Virtual Currencies at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

securities, fiat money and derivatives are held could become so relevant in the future that societies will need to regulate and supervise them more consistently.

Effective regulation requires a suitable addressee against which the rules can be enforced. In the case of virtual currencies, such as *Bitcoin*, it appears difficult or well-nigh impossible effectively to regulate the person or persons controlling the software (which I here call the 'software platform provider') as they are typically informally associated individuals that may be scattered around different jurisdictions.[70] Regulators could therefore attempt to regulate these networks by forcing local Internet providers to block the relevant data traffic.[71] However, this approach is only partly effective and politically and legally difficult to justify in a democratic setting as long as equally efficient, less intrusive means are at the regulators' disposal. Against this background, regulatory initiatives at present target the intermediaries at the intersection between the virtual currency and the financial market, in particular the so-called virtual currency exchanges, ie those entities exchanging fiat money for virtual currency.[72] Regulators could take the same approach in relation to blockchain financial networks on which securities, fiat money and derivatives are held and transferred. However, it is moot whether this approach would suffice, in particular as there might be risks in this context that can only be addressed for a blockchain financial network as a whole. This structural aspect will be touched upon in the following subsections but will only be fully addressed in part five of this article, after the various material risks have been discussed.

Hence, the main focus of the sections that follow will be on the material scope of regulation. As soon as financial assets such as fiat money, securities or derivatives are held and transferred through blockchain financial networks, the regulatory perimeter will need to extend to many more areas than just money laundering. This is due, first of all, to considerations of (market) scale: for the time being, transaction volumes in virtual currencies are tiny compared to those in financial assets.[73] Then there is the question of interconnectedness: currently incumbent market participants, ie banks and other financial institutions, are likely to become nodes in blockchain financial networks and to administer their and their clients' financial assets on them.[74] Potential negative externalities rooted in the operation of the relevant blockchain network, as discussed in the following section, will immediately impact on those financial institutions and their clients. For instance, if a blockchain financial network was to produce unexpected outcomes because of a software bug or loophole, all financial institutions using this network would instantly face the same operational difficulties, and there would be no option to work around them

70 See De Filippi and Loveluck, n 27 above, 8-10; V. Lehdonvirta and R. Ali, 'Governance and Regulation' in UK Government Chief Scientific Advisor, *Distributed Ledger Technology: Beyond Blockchain* (2016) at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, 42.

71 Wright and De Filippi, n 22 above, 51.

72 EU Commission, n 69 above, 7; Lehdonvirta and Ali, n 70 above, 42. See New York State Regulation on Virtual Currencies, n 69 above, s 200.2(q).

73 Broadbent, n 15 above, 3.

74 See below 1102.

individually. Also, the connection to the real economy would become much more immediate since, unlike virtual currencies, financial assets embody claims against corporate and state debtors.

I will analyse the following issues in turn. First, blockchain financial networks may influence the stability of financial markets. Secondly, self-governance within a network may cause distortions that lead to discrimination against parties that are unable to adjust their behaviour. Thirdly, the possibility of transferring financial assets on blockchain networks may render anti-money-laundering measures and similar rules partly ineffective.

Resilience and financial stability

Blockchain financial networks, like traditional market infrastructures such as clearing and settlement systems or central counterparties, could become systemically important in the future. Their function in the market places them among these critical infrastructures. Blockchain financial networks would provide a service that would not be easy to replace should they fail to function properly, as they would provide for the constitutive records of financial asset holdings, act as a repository for a variety of important data and as the platform on which smart-contract-based derivatives are executed.[75] As networks linking a multitude of financial market actors, potentially of different types, they are also highly interconnected.[76] For all these reasons, such networks are destined to become important in terms of financial stability once they have attracted a certain volume of assets and a critical number of users. It might therefore be necessary to regulate blockchain financial networks in order to ensure that they are resilient and do not contribute to systemic risk but, ideally, help to reduce it. There are a number of relevant aspects which I will address in turn below.

Operational Soundness and Software Loopholes

The first concern is about the operational soundness and continuity of the relevant processes. Uncertainty as to the accuracy or availability of records or the correct execution of smart contracts could have significant repercussions for financial stability.[77] The relevant hardware, ie the node-servers, and the individuals operating it are ‘distributed’ throughout the network, independent from each other and not centrally controlled – hence any concerns regarding integrity, availability, continuity, safety and accuracy relate to the software platform. Given its crucial importance for the nodes and their clients and for the market as a whole, there is a need for relevant regulation.[78]

However, this issue extends far beyond the operational functioning of the network. A matter of equal importance is that the processing of transactions and

75 See Bank for International Settlements, Committee on Payment and Settlement Systems, ‘Principles for Financial Market Infrastructures’ April 2012 at http://www.bis.org/cpmi/publ/d101a.pdf, paras 1.3, 1.15 and 2.2.
76 *ibid*.
77 *ibid,* Principles 15-17. See Peters and Panayi, n 2 above, 9-12.
78 See New York State Regulation on Virtual Currencies, n 72 above, s 200.16.

the execution of smart contracts must result in the 'correct' or 'true' outcome. What is correct or true is not defined objectively according to absolute criteria obtained outside the network. Rather, the yardstick is consensus among nodes on how transactions should be processed and records kept. This consensus is typically established when nodes join the network and thereby adhere to the rules determining the acquisition and disposition of assets and the execution of smart contracts on the network (hereafter referred to as 'internal rules'). These rules are laid down directly in the form of a computer code; there are no 'bylaws' or similar documents in human language.[79] The internal rules may also be changed following the relevant internal governance procedures.[80]

However, there is significant room for trouble. The software programming and user expectations may diverge, either because an unintended loophole, ie a planned software functionality that produces, in combination with other functionalities, unexpected results, has been created due to the sheer complexity of the software platform (as was the case with the *Ethereum*-DAO 50m USD 'theft', which did not, technically speaking, occur because of an illegal intrusion into the software but as a result of the exploitation of a previously undetected loophole in the software),[81] or because of a 'bug', ie a straightforward programming error.[82] *Ex ante* regulatory measures to avoid such loopholes or bugs are important also to ensure the transparency of the internal rules.[83] However, loopholes and bugs can never be entirely avoided and they might affect all or significant parts of the assets held in the network. Therefore, systemic stability requires that 'incorrect' results in a blockchain financial network be prevented before they materialise or that there is at least a possibility to reverse such results. The programmers of Ethereum, to the surprise of many, were able to 'reset' past transactions and undo the abusive transfers.[84] This approach obviously contradicts the original concept of immutable outcomes of blockchain-based transactions; however, as Ethereum has shown, it is necessary to protect the market at large from becoming hostage to a programming bug or loophole. Hence, it is questionable whether the original ideas regarding immutability will prove practicable as soon as blockchain technology is adapted for use in financial markets.

Risk Management

In any case, independently from the question of whether a blockchain financial network provides for the correct outcomes, it can contribute to systemic risk. Blockchain networks record the assets of their users. These assets are part of a highly complex risk management process in which every significant financial market participant is constantly engaged. Risk management is a central,

79 Lehdonvirta and Ali, n 70 above, 42.
80 See 1091-1093, below.
81 See text to n 67 above.
82 See European Parliament, n 20 above, para 2.a; Peters and Panayi, n 2 above, 10.
83 See European Parliament, *ibid*, para 2.f; Bank for International Settlements, n 75 above, Principles 8 and 11.
84 See text to n 67 above.

integral part of capital requirements regulation, and hence a centrepiece of the framework that governs financial markets.[85]

The main mechanisms used to mitigate risk are delivery-versus-payment, security or collateral, set-off, closeout netting and multilateral clearing of exposures. In addition, financial institutions hedge their market risks using derivatives such as interest rate swaps.[86] In principle, all these mechanisms could be programmed into the functionality of a blockchain financial network as smart contracts. However, in practice the technical hurdles are immense.

The key difficulty is that risk mitigation spans different classes of asset: for instance, a simple delivery-versus-payment mechanism keeps a performance (eg, a transfer of securities) on hold until the other party has likewise performed its part (ie made the corresponding cash payment), in order to release both at the same time, thereby eliminating the settlement risk. However, to do so requires both the securities leg and the cash leg of the transaction to occur in the same blockchain financial network, on pain of not being able to enforce the necessary interdependency with any certainty. Alternatively, if securities and cash were held in two different networks, both networks would need to be linked in operational terms.[87]

The risk management of a financial institution is a highly complex thicket typically managed with the assistance of computer algorithms. Cash, securities, claims and derivatives are all inextricably connected through the mechanisms mentioned above, ie delivery-versus-payment, security, collateral, closeout netting, clearing and hedging. Therefore, modern risk management requires all these asset types and mechanisms to be available in a single network. Such a universal network would obviously raise questions of systemic risk in itself. The alternative to such a 'leviathan'[88] would be to have several networks where different asset types could be perfectly and unalterably linked through these risk mitigation functions—however, the resulting set-up would probably be extremely complex, requiring a high degree of standardisation and interoperability so that ultimately such a meta-network of blockchain financial networks would resemble the current situation in terms of complexity and proneness to error.

Herding, Flash Crashes and Supervisory Stays

The unstoppable execution of transactions and smart contracts in blockchain financial networks might also have effects akin to systemic dangers provoked by the phenomena of 'herding' or 'flash crash'. The term 'herding' describes the synchronised behaviour of significant parts of the market as a reaction to certain

85 See Basel Committee on Banking Supervision, 'International Conversion of Capital Measurement and Capital Standards, Comprehensive Version' June 2006 ('Basel II', now integrated into 'Basel III') at http://www.bis.org/publ/bcbs128.pdf, 31-49.

86 See Bank for International Settlements, n 75 above, para 3.1.6.

87 Wall and Malm, n 3 above, 62.

88 B. Scott, 'Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain' E-International Relations, 1 June 2014 at http://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/.

market events. For instance, all hedge funds active in a given market segment may sell assets in the event of a sharply falling market, thereby amplifying the offending price movement. In extreme cases, herding may be one of the causes of so-called flash crashes, where extreme devaluation of an asset occurs in a very short period of time without any change in the underlying economic parameters. This phenomenon is typically due to identical behavioural patterns of the decision-makers or, where investment or risk mitigation decisions are outsourced to machines, to the use of algorithms that produce identical outcomes.[89]

The autonomous and unstoppable execution of transactions and smart contracts in blockchain financial networks may aggravate this phenomenon. Removing the human element entirely eliminates the last vestiges of elasticity in the behaviour of parties, which does to some degree exist in wholesale financial markets due to the generally relational character of contracting prevailing in this environment.[90] Eliminating elasticity may be advantageous from a market efficiency point of view in good times, but may also amplify market distortions in times of crisis.[91] Blockchain technology takes the 'immediateness' of market reactions to an extreme and may combine it with a high degree of interdependency of the various processes involved. This could, in addition, cause unwanted feedback loops, especially in relation to the operation of smart contracts that execute autonomously on the basis of market data automatically retrieved from data sources.[92] As a result, a single significant change in the market may immediately trigger another strong market move, which may in turn set off a third one, and so on. Hence, there is a need to assess blockchain financial networks and the potential of smart contracts in the light of rules addressing flash crashes and algorithmic trading.[93]

An additional issue is relevant in this respect: in order to be better prepared to prevent systemic risk caused by failures of banks or investment firms, recent legislation on bank resolution has established an administrative framework which is applied instead of judicial insolvency proceedings. Under this framework, supervisors are equipped with the authority to halt the execution of certain contract terms under certain circumstances and for a short period of time. The application of this 'supervisory stay' is intended to prevent the mass termination of derivatives and repurchase agreements in the event of failure of a bank or investment firm.[94] Automatic, unstoppable execution of

89 See Deutsche Bundesbank, 'Significance and Impact of High-Frequency Trading in the German Capital Market' Monthly Report, October 2016 at https://www.bundesbank.de/Redaktion/EN/Downloads/Publications/Monthly_Report_Articles/2016/2016_10_high-frequency_trading.pdf?__blob=publicationFile, 38-41.

90 See text to n 142 below.

91 *ibid*, 60.

92 See Peters and Panayi, n 2 above, 20.

93 See European Securities and Market Authority, 'Guidelines on Systems and Controls in an Automated Trading Environment' ESMA 2011/456, 21 Dec. 2011 at https://www.esma.europa.eu/sites/default/files/library/2015/11/2011-456_0.pdf, 32-49.

94 See Directive 2014/59/EU of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending [etc], Articles 69-71. It is debatable whether similar stays should also exist in insolvency proceedings, see P. Paech, 'The

blockchain-based transactions would produce the exact opposite.[95] In order to maintain the effectiveness of this administrative supervisory stay, the relevant authority would need to be provided with an 'emergency stop' function, enabling them to halt the automatic termination of contracts recorded in a blockchain financial network. Such functionality would need to be built into the smart contract itself, making the stay dependent on data input triggered by the relevant administrative decision.[96] By contrast, it would not be possible to allow the termination to happen and then afterwards 'reverse' it. First, because the termination would wipe out many derivatives and repurchase agreements that were important for the relevant bank's risk management and secondly, because it would be difficult to find counterparties prepared to offer new contracts to the near-insolvent party on economically viable terms.

Shadow Banking Risks and Bubbles

The emergence of blockchain financial networks and smart contracts may also influence the investment decisions made by market participants. Individuals or corporations may use the blockchain financial networks to store value, exchanging financial assets held with intermediaries for financial assets held in a blockchain network, in particular because of a perceived smaller risk, lower cost or better return as compared to more traditional ways of holding.[97] As such, a blockchain financial network could also assume functions resembling those typically performed by banks, notably that of storing money.[98] However, only the banks' clients benefit from the relevant safety nets, such as deposit guarantees and access to central bank money for liquidity support. Blockchain financial network nodes do not benefit from these safety nets. If they act as intermediaries for clients outside the network, these clients are only protected if the node is a bank and the clients' holdings are deposits or assimilated to deposits.[99] The negative impact of adverse events on the market as a whole may be amplified by the fact that retail customers could withdraw their savings from the traditional banking sector, thereby diminishing their liquidity base.[100] Both phenomena may cause risks comparable to those produced by so-called shadow banking.

Value of Financial Market Insolvency Safe Harbours' (2016) 36 *Oxford Journal of Legal Studies* 855.

95 See Raskin, n 43 above, 30.

96 *ibid*, 30; see text to notes 59-62 above.

97 See D. Awrey and K. van Zwieten, 'Law and the Shadow Payment System' Working Paper 26, September 2016 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843772, 24-27; E. Warnock and T. Mochizuki, 'Japan's Authorities Decline to Step in on Bitcoin' *The Wall Street Journal* 24 February 2014 at http://www.wsj.com/articles/SB100014240527023-04834704579402751676012112.

98 Awrey and van Zwieten, *ibid,* 27; see J. H. Rigsby, 'Virtual Currency, Blockchain and EU Law: The "Next Internet" in AML/CTF Regulation's Shadow' Lund University Masters thesis 2016 at http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8878538&fileOId=8878539, 9.

99 See New York State Regulation on Virtual Currencies n 72 above, se 200.19 (1)(a).

100 Broadbent, n 15 above, 3.

Taking this thought a step further, the use of blockchain technology and smart contracts may cause a false impression of zero credit risk, because smart contracts allow for the immediate and autonomous enforcement of collateral should the obligor fail to perform. Collateral takers might assume that they are free to take on higher exposures, for example to lend more money, as there seems to be no risk of unenforceability of the collateral.[101] This assumed certainty is risky in itself. Risk-takers will decrease their buffers in terms of reserves if they perceive a collateralised obligation to amount to zero risk. However, the uses of more efficient technology alone is poor justification for increased leverage in the financial system or, in other words, for stretching the liquidity cover of financial institutions even more thinly.[102]

Internal governance and discrimination

Bitcoin was originally conceived as a network comparable to a grassroots democracy. Its 'libertarian', anti-institutional motivation sat very well with the concept of a permission-less network open to all, where all information was public but users were generally anonymous, and where trust and mistrust were not an issue because strong cryptography and fail-safe processes made trust redundant. However, Bitcoin could not possibly have remained aloof in the long run from the ideology and private interests of its stakeholders and was progressively compromised by the social and cultural context in which the technology operated.[103] In particular, the validation of blocks and the associated creation ('mining') of new bitcoins has grown into a business that is today characterised by low margins and thus by a high degree of market concentration on a few very powerful players; as a consequence, there are a handful of Bitcoin mining entities or associations that effectively control the network and have a large say in its further development.[104] Also, a group of elite IT specialists run the system from a technical point of view, and these are effectively more influential than ordinary nodes given their superior knowledge and their role as gatekeepers between user consensus and computer code.[105] As a consequence, Bitcoin has evolved into a highly centralised network, ruled by an increasingly oligopolistic market structure.[106]

The internal governance of Bitcoin is, however, different from the internal governance of future blockchain financial networks set up by for-profit organisations such as banks, other financial institutions or Fintech companies. These networks will be set up either in a spirit of mutuality, assisting market participants to pursue common interests (in particular higher efficiency),[107] or as services provided to wholesale or retail customers. Still, once blockchain

101 See Raskin, n 43 above, 28: starter interrupters used to enforce security interests over cars might increase the volume of subprime auto loans.
102 Paech, n 94 above, 869-870.
103 De Filippi and Loveluck, n 27 above, 10.
104 *ibid*, 11.
105 *ibid*, 16, 18; Lehdonvirta and Ali, n 70 above, 42; see also n 67 above.
106 *ibid*, 16.
107 See above, 1079.

technology finds its way into financial assets and services, users may play different functional roles in the relevant networks, such as 'passive' nodes that do not contribute to the functioning of the network, or as 'active' nodes contributing resources such as computing power,[108] giving them less or more formal or informal influence on the relevant governance decisions. Nodes will also be dissimilar on other grounds, for example because they generate higher or lower transaction volumes, because they join the network at an earlier or later point in time, because they have different nationalities or reside in different territories, or because they may or may not participate in markets outside that particular network and, if they do, have different roles and importance there, too.

Very much as in any other type of network, these differences will influence the degree of bargaining power of the network nodes when it comes to the internal governance of the network. Mindful of the fact that financial institutions associated in blockchain financial networks, while they will have some interests in common, are nevertheless competitors at various levels,[109] bargaining power may be expected to be used to advance each node's own economic goals by influencing the internal governance of the network, behaviour that may generate decisions detrimental to other, weaker, nodes.

A blockchain financial network has several characteristics that are susceptible to discriminatory decision-making, thereby creating asymmetries within the network that could have a negative impact on the market as a whole. The most important such issue is that of actual access to a 'permissioned'[110] network, ie the possibility of excluding prospective new entrants or of only accepting them on unfair terms. Furthermore, processes and standards specific to the network, such as data formats or timelines, could be designed in such a way as to make it easier for some nodes to comply with them than for others. Also, the network could be designed to ensure that some nodes are able to extract more sensitive information about the dealings of their competitors than vice versa. Lastly, standards for reporting transaction data to supervisors could be set so as to make compliance with regulation easier for some nodes than for others. There may be other examples.

Such a situation may be acceptable from the public policy point of view so long as blockchain-based networks in financial markets do not become dominant.[111] However, once they do, these asymmetries can lead to competitive distortions.[112] Weaker nodes may be unable to adjust their behaviour, in particular for lack of alternatives. In that scenario, blockchain networks would come conceptually close to infrastructures underpinning the financial market, ie they would become akin to exchanges, settlement or payment systems. Such infrastructures, however, are subject to neutrality requirements in providing their

108 De Filippi and Loveluck, n 27 above, 14.
109 See B. McLannahan, 'Goldman Sachs quits R3 blockchain consortium' *Financial Times* 21 October 2016 at www.ft.com/content/598934e0-b010-11e6-9c37-5787335499a0 (last accessed 21 November 2016).
110 See text to notes 46-50 above.
111 Bank for International Settlements, n 75 above, para 3.18.2.
112 *ibid*.

services, even though they are currently for-profit organisations.[113] Hence, comparable rules would need to apply in the future to blockchain financial networks, ie they should have objective, risk-based, and publicly disclosed criteria for participation, permitting fair and open access.

Money laundering and other illegal activities

Beyond the spectacular cases of illegal or illicit use of virtual currencies,[114] concerns about money laundering and terrorist financing surfaced very early on, leading to relevant regulation in New York and intense debate in Europe and elsewhere.[115] Two characteristics inherent in blockchain technology considerably facilitate illegal activity. The first, and most obvious, is the possibility of transacting with a higher degree of anonymity than is afforded by account-based transfers,[116] with the instantaneous character of international transactions making it impossible to know who sends and who receives, for instance, a payment in bitcoins.[117] Secondly, even if blockchain-based networks were not generally anonymous, there would be no-one on hand to perform the functions that lie at the core of anti-money-laundering and related regimes.[118] In the 'real' world, that burden is placed on intermediaries, in particular banks and other financial institutions.[119] They are held liable for identifying the parties to a transaction, including background due diligence extending to beneficial ownership of companies. They must report suspicious transactions to the competent authorities and in certain circumstances may be banned from executing such transactions.[120]

In blockchain networks, intermediaries are not, in principle, needed.[121] There is a need for intermediation only where such networks intersect with the market outside. In the case of *Bitcoin* and other virtual currencies, users exchange virtual money for fiat money or vice versa through entities called exchanges.[122] As the virtual currency blockchain networks themselves are difficult to regulate, to date the exchanges are the most suitable entry points for regimes such as anti-money-laundering and counter-terrorist-financing laws,[123] even though this approach would leave out any part of blockchain activity that did not involve an exchange of currency, such as, for example, activities where

113 *ibid*, Principle 18.
114 See n 7 above.
115 See n 69 above; FATF/OECD, 'Virtual Currencies – Guidance to a Risked-based Approach' June 2005 at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf, 6; Mancini, n 7 above, 111-139; Rigsby, n 98 above.
116 See text to n 27 above.
117 EU Commission, n 69 above, 12; European Central Bank, Opinion CON/2016/49 12 October 2016 at https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2016_49_f_sign.pdf, 2; Rigsby, n 98 above, 31-32 and 37-38; Wright and De Filippi, n 22 above, 56.
118 Rigsby, *ibid*, 38.
119 *ibid*, 19.
120 See Directive (EU) 2015/849 of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing [etc], Arts 2, 4, 8 and 11.
121 Rigsby, n 98 above, 38.
122 See notes 70-72 above.
123 See n 115 above.

virtual currency is spent directly on goods and services.[124] Still, this approach requires the recognition of virtual currency exchanges as regulated entities, which itself creates a whole new, publicly recognised sector within the financial market, raising further regulatory questions. Under the circumstances, no common strategy has emerged so far.[125] There are no alternative ways of cracking down on illegal activity associated with state-remote networks by way of regulation. In particular, an outright ban seems to hold out scant promise as it is well-nigh impossible to enforce, except by blocking Internet traffic.[126] In other words, although there certainly seems to be a significant problem, no suitable solution has as yet been found.

As to future processing and recording of financial assets, in particular fiat money and securities, in blockchain networks, there is no room for a wait-and-see approach comparable to that taken towards virtual currencies.[127] Regulators would be sending the wrong signals and incentivising a move to the unregulated part of the market if new entrants were to be subject to no or more lenient—and therefore less costly—requirements purely on the ground that their business model was based on blockchain technology.[128] Hence, transfers of money and other assets through blockchain financial networks need to be subject to functionally equivalent rules preventing money laundering and other illegal activities. It will make less and less sense for regulation to address intermediaries at the intersection between the blockchain networks and the traditional financial market since, as financial assets are moved to blockchain networks, the role of such intermediaries is likely to decrease. In practice, individuals will be able to transfer fiat money and other assets directly through a blockchain network, requiring no intermediary, much in the same way as no intermediary is needed to pay for goods in a virtual currency.[129]

We are currently witnessing the creation of blockchain-based payment and money remittance services. The relevant service providers act as intermediaries, comparable to virtual currency exchanges in the Bitcoin context. They can be and are generally regulated.[130] As a consequence, they are suitable addressees for anti-money-laundering regimes and similar rules including user authentication (the so-called 'know-your-customer' or KYC requirement).[131] However, it needs to be clear who is responsible for applying these rules in cases where the role of intermediary is split or otherwise unclear, eg, in cases where blockchain-based remittance services rely on local stores to pay in and withdraw cash.[132] In that scenario responsibility can only fall to those controlling the platform, who therefore incur the full responsibility in terms of managing access and handling regulatory matters, as discussed below.[133]

124 Rigsby, n 98 above, 53.
125 See notes 72 and 97 above.
126 Wright and De Filippi, n 22 above, 56.
127 See EU Commission, n 69 above, 9.
128 *ibid*.
129 European Central Bank, n 117 above, 2.
130 See n 14 above.
131 Rigsby, n 98 above, 58; Wright and De Filippi, n 22 above, 54.
132 See, for example, www.goabra.com.
133 See below 1101-1102.

AUTONOMOUS ALGORITHMS AND PRIVATE LAW

One of the original traits at the basis of blockchain-based networks is that there is no trusted third person to effect and record transactions between nodes. In the world of blockchain, trust, which in the 'real' world is typically afforded to public authorities (such as the land register) or certain private parties (such as a bank or a notary), is replaced by reliance on software (see the second section above). For the nodes to be able to rely on their network's software, they must be convinced of its soundness, ie they must be confident that it allocates rights according to internal rules to which they agreed upon joining the network. At the same time, this principle entails that the process, once initiated, must be resistant to alteration and beyond human control. Otherwise, again, parties would need to trust the person controlling the process. As a logical consequence, the allocation of rights in blockchain financial networks must be unstoppable and irreversible.

However, the idea of such unstoppable and irreversible allocation *in practice* of individual rights to users creates tensions not only with the regulatory regime, as set out in the third part, but also with the private law framework. In the first subsection, I will discuss how the parties as well as the competent courts and regulators would lose authority over the enforceability of transactions or smart contracts once they were recorded on the blockchain. While the parties will themselves initially have agreed to this result, the second subsection will illustrate how their dealings may cause adverse externalities with regard to unrelated parties and the market as a whole, notably in respect of insolvency distribution and risk management. The authority to attribute rights in blockchain financial systems must therefore ultimately derive from the private law order, as explained in the third subsection.

The trust-less order and the loss of authority of the courts over transaction enforceability

A key component of blockchain is that the process of disposition and acquisition of assets and the execution of smart contracts is determined solely by the internal rules[134] of the blockchain network. The algorithms directly produce the relevant effects. In this process, the rules are constantly called upon to 'decide' whether or not a certain transfer will be executed or whether the right of a party arising under a smart contract will be automatically enforced. However, in taking this 'decision', the software typically attributes rights to one party that it takes away from the other party. For instance, a smart derivatives contract might include a functionality causing it to terminate itself upon default or other types of termination event, automatically calculating and enforcing the amount still due from one party to the other, while at the same time transferring the associated collateral to the party that is 'in the money'.

Where the other party feels that the conditions for termination were not actually met it may decide to go to court. Where transactions are

134 See text to n 79 above.

near-anonymous, as they are in first-generation blockchain applications, the story typically ends here as there is no *de facto* way of suing the other party for damages in kind or in money. Still, the parties may have previously agreed to an internal dispute settlement mechanism (which does exist, for instance, for online acquisitions paid with bitcoins).[135] This mechanism applies the rules of the system, but not general private law, and necessarily results in an outcome compatible with the logic of blockchain networks—which means that validated transactions and the execution of smart contracts cannot be undone on the record.[136]

Even in permissioned systems, where the identity of users is known,[137] court decisions do not exert the same authority as in the traditional context of financial market transactions. Should a party claim that a transaction or smart contract that was executed under the internal rules of the network was unenforceable, the court will first consider whether the parties have agreed to the application of the internal rules to their dealings,[138] as an expression of party autonomy, or even as a form of *lex mercatoria*.[139] In that case, the code, or rather how it is understood in human language, would be the law, and every subsequent transaction would occur in accordance with it. In other cases, the court may hold that as a matter of general private law the transaction was unenforceable, eg, because there was no valid agreement on the internal rules, or in case of a lacuna.

However, even presupposing that there was a trusted entity controlling the network to whom the relevant court order could be addressed, the court will still be unable to order a rectification of the blockchain, as the record cannot be changed subsequently without destroying the logic of the trust-less network itself.[140] The only remaining possibility is to claim damages from the transferee, in kind (ie the court may order the initiation of a new, reverse transaction) or in money. However, as is the case in traditional financial markets, claiming damages will often frustrate the transferor whose interests were overridden, in particular if the transferee has become insolvent in the meantime, or if the transferor has an interest in the specific assets which have been transferred. Yet, as opposed to the traditional environment, where registers can still be corrected and transactions operationally reversed in certain cases, the blockchain environment offers damages as the only remedy, invariably subjecting the transferor to the risk of insolvency of the transferee.

This issue is also relevant in relation to smart contracts that are still open, where one party claims that the contractual duties should be adapted in response to new circumstances not previously considered by the parties, ie in case of a

135 See also Ortolani, n 35 above, 592-629.
136 *ibid*, 602, 611.
137 See text to notes 46-50 above.
138 Raskin, n 43 above, 22.
139 See Ortolani, n 35 above, 613-614. Wright and De Filippi, n 22 above, 45-50. Regarding cross-jurisdictional settings see below, 1103-1108.
140 See Peters and Panayi, n 2 above, 15. See also New York State Regulation on Virtual Currencies, n 72 above, s 200.19: clients have to be informed that transactions may be irreversible including in cases of fraud or error and that technical difficulties experienced by the service provider may prevent the access to the user's virtual currency units.

lacuna.[141] In the original blockchain setting, there is no way of changing the record, and thereby the contract,[142] even in cases where both parties agree to the change. To revert to our earlier example: in the event of default in the context of a derivatives contract, the non-defaulting party too may often prefer not to terminate the contract and instead choose implicitly or expressly to adjust it, in particular by granting a grace period. Again, for lack of a trusted entity with the authority to change the record according to the parties' agreement, the terms of the smart contract cannot be changed and its execution cannot be halted. A subsequent 'reversal' of the termination, by entering into a new contract, as a form of damages in kind, will often not be possible as the circumstances may have changed in the meantime, in particular where one of the parties has become insolvent or where market conditions have undergone considerable change.

Thus, any kind of *ex post* review is limited to the potentially unsatisfactory possibility of claiming damages in court. Here, blockchain-held assets differ markedly from assets held in more traditional, account-based structures. Current financial market infrastructures, such as clearing and settlement systems, also use computer programmes to prioritise their users' interests on the basis of their internal rules, as described above.[143] However, outcomes can still be changed by the infrastructure operator, honouring the agreement of the parties or court orders, or simply correcting operational failures.

Raskin argues that the precision of the programming language removes some of the potential need for *ex post* review, as the internal rules and in particular warranties and conditions can be formulated with much greater accuracy.[144] However, while this may indeed remove linguistic ambiguity, the greater precision is of little help in relation to issues such as changing circumstances, lacunae or even, depending on the applicable law, questions of equity or good faith.[145] Rather, these issues could be addressed by leaving certain parts of the agreement outside the blockchain record as a 'non-smart' and thus modifiable contract, whereas other parts might 'go smart' and be self-executory and immutable, thereby building some flexibility into the relevant agreement.[146] Alternatively, the code of the smart contract could become more granular, in an attempt to address all potential future circumstances that may have an impact on the contractual duties—an approach which, of course, may come close to, but ultimately will never achieve, perfection.

Third party effects and regulation at the intersection with private law

The loss of control over the enforceability of rights is, in principle, acceptable in so far as the parties to a blockchain-based transaction and other users of that blockchain network are concerned. By adhering to the network, they have,

141 Werbach, n 10 above, 65.
142 *ibid,* 22; Wright and De Filippi, n 22 above, 26. See also text to n 90 above.
143 See Directive 98/26/EC of 19 May 1998 on Settlement Finality in Payment and Securities Settlement Systems, Art 2(a).
144 Raskin, n 43 above, 21, 22. See also Wright and De Filippi, n 22 above, 24-25.
145 See Raskin, *ibid*, 22.
146 *ibid*, 24.

implicitly or explicitly, agreed to operate in a technical, trustless environment, which only relies on maths and cryptography,[147] and accepted that the internal rules determine the outcomes of their dealings.[148] However, the effect on third parties outside the relevant blockchain network and on the market as a whole is more problematic.[149]

The starting point is the question of whether relevant assets held in a blockchain financial network still belong to the insolvent estate, and hence are available to its creditors, or whether they are outside of it, notably because they have been validly transferred to an acquirer.[150] What constitutes an asset of the insolvent is determined primarily by the general principles of property and contract law applicable to solvent parties.[151] Hence, the internal rules of the blockchain network apply, still subject to certain rules from which parties cannot derogate, eg, requirements for valid assignment or for perfecting security interests. However, since the rights of the insolvent's general creditors (who are third parties unrelated to the blockchain network) are at stake, the court will also apply certain mandatory rules protecting the insolvent estate against an outflow of assets or guaranteeing the *pari passu*[152] treatment of creditors.[153] Hence, parties may be surprised to find a court or insolvency official avoiding transactions that have occurred within the blockchain financial network, and trying to 'claw back' the assets acquired much earlier in breach of these rules, or claiming damages.

Ortolani argues that in similar contexts, enforcement outside the court system on the basis of autonomous rules can be an efficient way of settling divergences of this kind, citing the case of attribution of Internet addresses by ICANN.[154] This practice may seem acceptable in respect of Internet addresses, however, financial assets, as opposed to Internet addresses, are constantly traded and encumbered, ie they may, until insolvency strikes, continuously enter and leave the estate. In other words, when it comes to financial assets there is a much greater need to establish whether such earlier transactions occurred in breach of the *pari passu* or similar rules.

147 De Filippi and Loveluck, n 27 above, 7.

148 See Raskin, n 43 above, 24.

149 *ibid*, 25.

150 Bank for International Settlements, n 75 above, para 3.1.6.

151 R. Goode, *Principles of Corporate Insolvency Law* (London: Sweet & Maxwell, 2011) 6-01. The question of which law is applicable in international settings is addressed in the fifth part of this article.

152 For ease of reference, this article adopts a broad understanding of *pari passu* as the principle of equal treatment of general creditors which informs three questions, notably which assets are available for distribution, who participates in the distribution and how the assets should be shared amongst the general creditors (notably pro rata). However, these three issues differ conceptually, see, for example, M. Bridge and J. Braithwaite, 'Private Law and Financial Crisis' (2013) 13 *Journal of Corporate Law Studies* 361, 367-370.

153 For example, in England, undervalue transactions or preferences can be avoided if they occur within a two-year period prior to insolvency in the case of a beneficiary that is connected with the debtor company, or within six months in the case of an unconnected beneficiary, see Insolvency Act 1986, ss 238, 239 and 240. For an overview of the differences in avoidance rules from an international perspective, see Paech, n 94 above, 861-867.

154 See Ortolani, n 35 above, 604-605. ICANN is the Internet Corporation for Assigned Names and Numbers and holds the monopoly over Internet addresses.

Looking at the issue from the perspective of the solvent counterparty, other uncertainties become visible. Risk mitigation in financial markets is largely based on legal devices such as security, collateral, contractual termination, set-off and close-out netting, which generally feature in the parties' contractual agreements. The effectiveness of risk mitigation depends on whether these contractual rights are enforceable as soon as the other party becomes insolvent. It is, however, unclear whether a court would regard these rights as enforceable where they arise from a smart contract recorded in a blockchain financial network. The fine balance established between contractual risk mitigation tools and mandatory insolvency law, as typically codified in so-called safe harbour rules, is very fragile.[155] It has to reconcile contractual freedom with the interests of third parties and jurisdictions have typically adopted a strict line of policy in this respect. There is a significant danger that a court may consider this balance distorted if the strict mechanical execution of the stipulated contractual risk mitigation mechanisms in a blockchain financial network diverges, even if only slightly, from what is deemed acceptable generally. Contractual risk mitigation devices might be unenforceable as a consequence, derailing both parties' risk management.

This issue extends beyond private law into the sphere of financial regulation. Regulation attaches crucial importance to the enforceability of contractual risk mitigation, such as collateral, set-off and close-out netting. In particular, capital requirements are calculated on the basis of the net risk, ie the risk that remains after risk mitigation devices have been taken into account. Risk mitigation mechanisms can reduce a financial institution's risk by up to 80 per cent.[156] However, their risk-mitigating effect is only recognised under the Basel Accords and other regulatory texts to the extent that enforceability can be guaranteed *ex ante*—in practice, financial institutions have to prove enforceability by providing reliable legal opinions to that effect.[157] Otherwise, risk and, accordingly, capital requirements must be calculated on a gross basis, which the financial sector cannot afford. As a consequence, not only may private-law-based risk mitigation tools fail when they are actually needed, ie in the event of insolvency, but the uncertainty regarding the enforceability of these tools may also unravel any risk-focused regulatory regime such as, in particular, capital requirements linking back to questions of systemic stability, as discussed earlier.[158]

Connecting internal rules to mandatory law

The somewhat troubling outcome of the discussion above is that, on the one hand, the internal rules, in accordance with party agreement, produce

155 See Paech, n 94 above, 861-866; Bank for International Settlements, n 75 above, para 3.1.6.
156 See Bank for International Settlements, 'OTC Derivatives Statistics at End-June 2016' November 2016 at http://www.bis.org/publ/otc_hy1611.pdf, 11, 14: the credit exposure is only 18% of the gross market value due to enforceable set-off and netting arrangements (collateral not taken into account).
157 See Basel Committee on Banking Supervision, n 85 above, para 188a.
158 See above, 1087-1088.

results that cannot be changed subsequently, save, at best, through claiming damages. On the other hand, the internal rules cannot displace mandatory law, in particular the insolvency avoidance rules or the prerequisites for a valid assignment or for perfecting security interests, which as a consequence still apply and may lead to unenforceability of transactions. However, the law cannot leave this obvious friction unaddressed and needs to bring the outcome under internal rules of blockchain financial networks into harmony with the relevant law. The neatest way is to recognise the operation of internal rule in the law itself.

This can be achieved by expressly recognising the outcome under the internal rules of a blockchain financial network as enforceable against third parties. However, this effect can only be granted to networks on condition that the relevant internal rules of the network treat dispositions and acquisitions so as to be compatible with general principles of law, actually making them a vehicle for the law. In particular, outcomes may not be arbitrary but instead must be based on objective criteria, such as chronology, publicity and specificity. In relation to insolvency avoidance, the law should recognise the reality of the immutable record and state that transactions on a blockchain financial network, once initiated, cannot be unwound or reversed by the blockchain network, unequivocally referring parties to a claim for damages as the only remedy.

The relevant legal provisions need to be statutory, in order to rank equally with the mandatory provisions they seek to address. Such rules do exist at the moment, notably in respect of the enforceability of acquisitions and dispositions as the outcomes of automated clearing processes for cash or securities, generally called 'finality'.[159] These rules can serve as blueprints for legal provisions connecting the internal rules of blockchain financial networks to mandatory rules of law.[160]

Secondly, and this is the more difficult part, accepting outcomes as enforceable *generally* means that there might still be exceptional circumstances, think of the Ethereum case, that cast doubt on whether the execution can actually be backed by private law, even if the internal rules are generally deemed to be in line with it. For instance, a software loophole may produce a result that is incompatible with the principles underlying the network rules, which are, in turn, recognised by the law. The network itself may function correctly but the market environment may be derailed as a consequence of the unexpected outcome.[161] The fact that the enforceability of acquisitions is supposed to be in harmony with the law somehow suggests that there must still be a way of undoing transactions and changing the blockchain, if only in exceptional circumstances. In other words, as soon as financial assets are held in blockchain financial networks, the law needs to give guidance on how to handle an incident of the Ethereum type wherever networks administering financial assets are concerned.

159 EU Settlement Finality Directive, n 143 above, Arts 3-7.
160 See European Parliament, n 20 above, para 18.
161 See text to notes 66-67 above.

DETERMINANTS FOR A GOVERNANCE FRAMEWORK

The preceding two parts identified a number of open questions in areas where the character of blockchain financial networks presents specific challenges to financial regulation and private law. As discussed earlier, the concept of blockchain is still evolving and different types of network will pose greater or smaller challenges in terms of governance, and some types may even be entirely unproblematic in this respect.[162]

However, legal and regulatory arrangements cannot be tailor-made for each blockchain network. Therefore, in the following, I will discuss two central issues that cut across the 'material scope' of regulation and private law discussed earlier, in particular the structure of blockchain financial networks and the importance of the cross-jurisdictional view. These two aspects are the main determinants for the effective design and implementation of a regulatory and legal framework capable of governing different types of network.

Structure of the network

The preceding two chapters have shown that blockchain financial networks need to be regulated on several counts, and that ultimately private law needs to apply within these networks. But how can regulation and private law be extended to blockchain financial networks in the most efficient manner? Disintermediation, leading to the abolition of accounts and intermediary-client relationships more generally, will render traditional regulatory strategies largely inefficient and remove an important element to which private law rules traditionally attach. Instead, we must focus on what actually replaces the two-party relationship: a distributed network, built on poly-directional relationships among its nodes, which are linked solely through a software platform. Hence, regulation and law could target the software platform or the nodes, or both.

Platform providers[163] for first-generation blockchain applications are generally informally organised groups of individuals. Today, Fintech start-ups, well-established financial institutions and infrastructures, and even central banks may venture into setting up blockchain financial networks. There are a number of regulatory and legal aspects that can only be addressed for a blockchain financial network as a whole, regardless of how the circle of nodes is made up. The platform provider is the only suitable point of entry for network-wide regulatory and legal rules.[164] Starting from basic requirements regarding safety, availability, integrity and continuity of service, any rules that can only be implemented centrally must be imposed on the platform provider. As a consequence, platform providers need to be legal persons (natural persons are too elusive) regulated by the state. There may still be state-remote, unregulated blockchain networks where the platform is provided under a more informal arrangement, such as for Bitcoin or Ethereum. However, it should be impossible to issue securities through these networks and they should not be dealing with fiat money. To

162 See text to notes 17-21 above.
163 See text to n 70 above.
164 Lehdonvirta and Ali, n 70 above, 42, 43.

achieve this goal, it is not necessary to close them down or block access to their websites. It is sufficient to prohibit regulated financial institutions from dealing with such networks.

Platform providers have to ensure the soundness and continuity of the software platform.[165] Most importantly, this includes aligning the internal rules governing the acquisition of rights and the execution of contracts with private law.[166] Turning the spotlight onto issues of systemic stability, the platform provider has to help prevent flash crashes and bubbles, not only by shaping the software accordingly but also by providing for relevant reporting mechanisms.[167] Furthermore, in case of a permissioned network,[168] the platform provider must administer admission to the network,[169] ensuring non-discriminatory access to it[170] and respecting relevant restrictions as to the circle of users or as to territorial reach.[171]

Whether the platform provider should be the addressee of *all* relevant regulatory or legal rules depends on who the nodes of the blockchain network are: if the circle of nodes consists exclusively of regulated financial institutions (which may act as intermediaries and therefore maintain account-based relationships with clients[172]), the regulatory burden can be shared between them and the platform provider. In this case, regulatory and legal rules that do not need to be implemented centrally are addressed to nodes.[173] Generally, regulated financial entities will already be subject to relevant rules, such as an anti-money-laundering regime. However, relevant nodes must be authorised for the specific type of service provided by the network. For instance, if the network provides payment services, nodes authorised as banks will automatically be subject to all relevant regulation. Conversely, in a network administering securities, nodes authorised as payment services providers alone are not sufficiently regulated.

Where the nodes of a given network are entities not regulated as financial institutions, or individuals, the situation is completely different. In this case, there are no intermediaries that could apply relevant regulation to their relationships with clients. The only entity capable of applying the relevant regulation to the network and its nodes is the platform provider itself. In that situation, the platform provider would need to be the addressee of the full range of relevant regulatory and legal rules, thereby becoming a fully regulated financial institution itself which does not,[174] however, maintain accounts with its nodes but controls the network through means of access control and programming of the network software.

165 See above, 1086-1087.
166 See above, 1097-1100.
167 See above, 1088-1090.
168 See text to notes 46-50 above.
169 See above, 1091-1092.
170 See above, 1093.
171 See below, 1103-1104.
172 See text to n 29 above.
173 See New York State Regulation on Virtual Currencies, n 72 above, s 200.8 (capital requirements), s 200.9 (custody and protection of customer assets), s 200.15 (anti-money laundering rules), s 200.19 (consumer protection); European Commission, n 69 above, 7.
174 See Bitstamp at www.bitstamp.net/payment-institution-license/.

Thus, 'structure' as the first determinant refers to who the nodes of a network are and what services it provides. As a rule of thumb, the application of regulatory and private law rules to blockchain financial networks requires less adaptation of existing rules to the extent that such networks are homogeneous as regards their circle of nodes and the services provided. For example, a network specialising in payments that has as its nodes only authorised payment service providers or banks will not pose any great problem from the point of view of regulation and private law. By contrast, a network for clearing securities transfers against cash settlement that also offers collateral management and has both non-financial corporations and regulated financial institutions as its nodes will be significantly more complicated to govern.

Domestic and cross-jurisdictional reach of networks

Financial markets are highly internationalised, whereas their governance is still largely defined on the basis of territorial criteria. States exert regulatory and supervisory authority over the activity of financial institutions on their territory, and the law governing dealings between market participants can only be chosen to some extent, being imposed on the basis of territorial considerations for a number of important issues. Therefore, the effective governance of blockchain financial networks requires a strategy explaining how the regulatory and legal solutions, which are limited in their territorial reach, can be applied to networks that are potentially spread across several countries. This paper has already shown that issues of regulation and private law are inextricably linked in some respects.[175] This linkage is also an important element in overcoming the discrepancy in terms of the reach of a blockchain network and the means of governance. In particular, the enforceability of rights must be made dependent on the effective regulation of the relevant blockchain network in its own jurisdiction. I will first look at the public law side of the issue before turning to private law questions.

Cross-jurisdictional Regulation and Supervision

Access to internet-based financial services is difficult to contain and control by local supervisors. They may be unable to regulate and supervise a service effectively because the platform provider and the nodes are not located in the same jurisdiction.[176] Outright prohibitions are theoretically possible but difficult to justify—investors are ultimately free to risk their own money—and hold out scant promise of effective enforcement unless online access is blocked.[177] Mechanisms to dis-incentivise the use of foreign blockchain financial services are probably more efficient—here, regulatory approval of certain blockchain financial networks can of itself be such an incentive.

175 See above, 1087-1090.
176 Wright and De Filippi, n 22 above, 20-21.
177 *ibid*, 56.

Many blockchain financial networks will aim at an international, or even global, circle of users. However, being regulated in one jurisdiction does not generally satisfy regulators in other jurisdictions. The EU is in an exceptional position in that it has an effective common framework already in place: the EU 'passport' is linked to the authorisation and continued supervision of financial services providers in their home Member States and is in principle also good for providing the same service in other EU jurisdictions.[178] A blockchain financial network, through its platform provider, could be a beneficiary of the passport, which argues very much in favour of having a platform provider authorised as a financial institution of the relevant type, eg, as a payment service provider.[179]

Outside the EU, mutual recognition of authorisation and other supervisory decisions is close to anathema. As a fall-back option, a blockchain financial network could remain restricted to nodes within one jurisdiction, or seek authorisation in all jurisdictions relevant for its business. Alternatively, the market could be restricted to countries that do not require providers of the relevant service to be licensed (which would largely exclude the US and the EU, as they have regulatory regimes in place for just about every kind of financial service). Neither solution is conducive to innovation. However, at the moment, there seem to be no alternatives and blockchain financial networks will need to go through the motions of obtaining multiple authorisations. A set of international standards, which could borrow rules from texts developed for other types of market infrastructure,[180] would serve regulatory convergence and thus facilitate the authorisation process for blockchain financial networks seeking to establish themselves in several jurisdictions.

Obviously, this is a highly sensitive issue for London-based financial innovators should the UK leave the EU internal market as a consequence of the imminent termination of its EU membership. UK-based financial service providers will lose their passports and be treated as third country entities. They may decide to establish a locally incorporated and supervised subsidiary in an EU-27 State that would then allow them to benefit from an EU passport. Still, for UK entities, the process of authorisation would be facilitated as long as the relevant UK rules are in line with EU rules—however, this is an advantage that, after the loss of passporting privileges, would need to be formalised under a separate regime certifying equivalence of standards on a case-by-case basis.[181]

178 See European Banking Authority, 'Passporting and Supervision of Branches' at https://www.eba.europa.eu/regulation-and-policy/passporting-and-supervision-of-branches.
179 See above, 1001-1002 and n 174 above.
180 See Bank for International Settlements, n 75 above.
181 See European Commission, 'Equivalence with EU Rules and Supervision' at http://ec.europa.eu/ finance/general-policy/global/equivalence/index_en.htm; 'Equivalence Decisions taken by the European Commission' at http://ec.europa.eu/finance/general-policy/docs/global/equivalence-table_en.pdf.

Cross-jurisdictional Co-ordination of Private Law

The international framework supporting the enforceability of financial assets in foreign jurisdictions is rudimentary and non-binding.[182] There is a binding, albeit fragmentary, private law framework covering this area in place in the EU, which despite some harmonisation of aspects of substantive law is built on a conflict-of-laws solution. This means that domestic laws continue to apply under a conflict-of-laws regime that co-ordinates their application.[183] More ambitious international harmonisation of the legal framework for assets and contracts recorded in a blockchain network is unlikely to happen, particularly where the harmonisation of mandatory law is concerned.[184] Rather, autonomous national laws, ideally coordinated by a set of global principles, key attributes or some other type of benchmark will retain their authority over such assets and contracts.

Such a framework would involve three main threads, which I will address in turn below. In particular, it must be possible clearly to identify the law of *which* state is to apply to the assets held and smart contracts recorded in a blockchain financial network; the law so identified should determine the validity and enforceability of these assets and contracts *also* in foreign insolvency proceedings; and, for both of these, the jurisdiction of the applicable law must follow a number of standards regarding the legal and regulatory treatment of blockchain financial networks.

Applicable Law

The enforceability of a right in a financial asset depends on the law applicable to that concrete right, which, in turn depends on the legal nature of the relevant asset. However, there is little international compatibility as to the legal nature of even the most common financial assets. The right of an investor in non-corporeal securities electronically held in accounts is a case in point, as it is regarded as beneficial ownership in England, whereas most other jurisdictions classify the right of the investor as 'full' property in securities or shared property in a pool thereof, or as an insolvency-proof claim against the relevant intermediary with no legal connection to the underlying securities.[185] Another example are registered shares, which are *choses* in action in English law, for which, however, no corresponding concept exists in many other jurisdictions,

182 Convention on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary (Hague Securities Convention) at www.hcch.net/index_en.php?act=conventions.text&cid=72; Unidroit Convention on Substantive Rules for Intermediated Securities (Geneva Securities Convention) at www.unidroit.org/english/conventions/2009intermediatedsecurities/ main.htm; UNCITRAL Model Law on Secured Transactions (2016) at www.uncitral.org/pdf/english/texts/security/ML_on_ST_ebook.pdf.

183 Settlement Finality Directive, n 143 above, Arts 8 and 9; Directive 2002/47/EC of 6 June 2002 on Financial Collateral, Art 9; Regulation (EC) 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I), Articles 3, 8 and 17.

184 Paech, n 25 above, 1.

185 See J. S. Rogers, 'Policy Perspectives on Revised UCC Art 8' (1995-96) 43 *UCLA Law Review* 1449; L. Afrell and K. Wallin-Norman, 'Direct or Indirect Holdings – A Nordic Perspective' (2005) 10 *Uniform Law Review* 277; F. Nizard, *Les titres négociables* (Paris: Economia et Banque Revue, 2003) 245-252; J. Benjamin, *Interests in Securities* (Oxford: OUP, 2000) 3-59.

which may classify them as property in a movable, or *rights in rem*.[186] By the same token, the right to money in a bank account, under English law, is a personal claim that can be traced to an onward acquirer and therefore has a proprietary trait,[187] whereas it has no proprietary attributes in other jurisdictions.

Cutting through this thicket merits a study of its own,[188] but the point I wish to make here is that no international blockchain financial network can work if every jurisdiction involved were to classify the asset held in the network in accordance with its own idiosyncratic criteria. At present, international transfers of financial assets operate through accounts, ie they are two-party relationships, and a court would determine the nature of the right in question according to the law that applies to that specific account.[189] However, in blockchain networks, there are no accounts,[190] hence the question of which law applies to a right in an asset or flowing from a contract needs to be defined for the entire network *en bloc*.

Following the *lex rei sitae* rule, the law applicable to assets and rights held in a blockchain network would be that of the location of the nodes. As this would lead to the application of different laws within the network, this approach is excluded. The alternative approach of *lex societatis* (in the case of shares) or *lex contractus* (in the case of bonds) may likewise result in the application of different laws within a network. Hence, the only suitable solution is to define that law for the network as a whole and to do so from the outset, either as a function of the jurisdiction that regulates the platform provider and hence the network, or on the basis of the initial choice of law made by the platform provider. That law would then flow into the design of the internal rules of the network, determining how assets are transferred and rights are executed. However, in order to avoid forum shopping, the choice of law should be restricted, in particular to jurisdictions where the platform provider is incorporated or has a major operation.[191] This approach is also followed by the EU Settlement Finality Directive, following which only the law of a Member State can be chosen to govern the rights within the system.[192] Hence, as a consequence of 'Brexit', English law may in the future be ineligible for settlement systems operating in the EU. Should the EU legislate in respect of blockchain financial network, it seems likely that, as an analogy, the choice of law will be restricted in a similar way. Hence, from an EU perspective, English law could not be chosen as the law governing the relevant rights.

186 See J. Benjamin, *Financial Law* (Oxford: OUP, 2007) para 3.22.

187 *Foley* v *Hill* (1848) 2HLC (HL) 36 *per* Cottenham LC; *Foskett* v *McKeown* [2001] 1 AC 102, 108-109, 126-129 *per* Millet LJ; see T. Cutts, 'Tracing, Value and Transactions' (2016) 79 MLR 381, 384.

188 See Paech, n 25 above, 1-19.

189 See Financial Collateral Directive, n 183 above, Art 9; Settlement Finality Directive, n 143 above, Art 9; Hague Securities Convention, n 182 above, Art 4.

190 M. Kalderon, F. Snagg and C. Harrop, 'Distributed ledgers: a future in financial services?' (2016) 31 *Journal of International Banking Law and Regulation* 243, 247.

191 See Hague Securities Convention, n 182 above, Art 4(1).

192 See Settlement Finality Directive, n 143 above, Art 2(a) second indent, Art 9(2).

Recognition Under the Lex Fori Concursus

The acid test, however, is whether the relevant rights are also enforceable should one of the nodes become insolvent. In that case, enforceability is traditionally determined by the *lex fori concursus*, typically identified on the basis of a location-based connecting factor. As a result, the *forum* could be the jurisdiction of any of the nodes of a blockchain network.[193] To achieve legal certainty as to the enforceability of the rights, it would be crucial for all these jurisdictions to consider enforceability on the basis of the law of the network, also in the event of insolvency of the relevant node.

However, this is not a given. While the courts in insolvency proceedings will generally recognise the enforceability of earlier acquisitions and dispositions of the insolvent and of the contracts into which it has entered, even if these are governed by a foreign law, there are stark differences as to detail. In particular where courts feel that a specific arrangement impinges on the equal treatment of creditors (*pari passu* principle) as understood by their own law, they may regard the rules of their own jurisdiction as mandatory and any diverging effect under a different law as unenforceable.[194] Whereas outright dispositions and acquisitions are typically not particularly ambiguous, and contractual rights to performance generally accepted, difficulties may arise where the parties arrange for security (such as a pledge, mortgage, or lien) in assets held in a blockchain network, where financial collateral is provided (including mechanisms such as margining, substitution and right of use), or where contractual termination rights, set-off or close-out netting are stipulated.[195]

These issues are as a rule problematic in international settings, and much of the legal detail to be considered in the context of risk mitigation is owed to these jurisdictional differences. The financial industry has learned to manage the legal risk involved, notably commissioning legal opinions covering all relevant scenarios to achieve an acceptable degree of *ex ante* legal certainty. However, in a scenario involving an international blockchain financial network, this approach will probably be less effective. At present, a party considers its risk in two-party relationships (with the counterparty, and with the intermediaries holding or transferring the relevant cash and securities, including collateral). If the relevant rights are enforceable in insolvency, the risk is considered acceptable. This 'risk architecture' will be changed where a blockchain financial network is involved. The enforceability of rights held in the network becomes the point of reference; however, each jurisdiction will develop its own conditions as to the enforceability of assets and contracts held in a blockchain network. In principle, the problem is not in any way structurally different from the legal uncertainties currently faced by the financial industry in cross-jurisdictional situations. However, it will remain unclear for quite some time which path legislators and courts will take, leading to uncertainty in the transition period. The financial industry will be unable to address the uncertainty arising from

193 See Bank for International Settlements, n 75 above, para 3.1.11.

194 *ibid*; P. Paech, 'Close-out Netting, Insolvency Law and Conflict of Laws' (2014) 14 *Journal of Corporate Law Studies*, 419, 431-432; see Rome I Regulation, n 183 above, Art 8 and 17.

195 See Paech, n 102 above, 861-867.

the shift towards assets and contracts recorded in international networks as long as the legal framework is unclear.

The best solution in terms of supporting changes to statutory laws is to agree among jurisdictions that assets and contracts recorded in a blockchain financial network are enforceable also in insolvency, and that this is subject to the limitations set by the law governing the network, rather than by the limitations set by each *lex fori concursus*. Thus, nodes would not need to worry about the specificities of the insolvency laws in all jurisdictions where fellow nodes are located, but only about the limits imposed by the law that governs the network and its internal rules.

Trading Enforceability in Return for a Common Regulatory Standard

This solution is, however, politically sensitive because the *lex fori concursus* would lose authority over the policy-laden aspect of creditor protection in insolvency. Contractual derogation from this core area of insolvency law is, as a rule, impossible.[196] However, by accepting that the law that governs the network overrides the local insolvency law, nodes are somehow given the option, if not to derogate from insolvency law altogether, to choose the insolvency law of another country in respect of the assets held in the blockchain financial network. There are precedents in EU law,[197] which could serve as a model.

Yet the possibility of derogating from local insolvency law in favour of a foreign law would be highly significant, as it potentially concerns a large part or even all of an insolvent's assets and contracts held in a blockchain network. Hence, it may not be possible to envisage such a shift unless all jurisdictions concerned agree on common standards for regulating blockchain financial networks. As shown in the preceding two parts, risk-based regulation and private law enforceability are closely linked, so that such standards would also extend to the regulation of the internal rules of the network governing the acquisition and disposition of rights and the execution of contracts. Only if jurisdictions were to agree on such a common standard might the concession of a chosen insolvency law be acceptable from an insolvency policy point of view. Regulation and private law would thus result in a closed system on the international scale, as they typically do domestically.

CONCLUSION

Financial market activity conducted through blockchain networks poses risks very similar to those existing in the current, intermediary-based market: there are issues regarding resilience and financial stability, market distortion and illegal activity. At the same time, a future blockchain environment will face private law questions similar to those the market faces now, in particular regarding the enforceability of rights in insolvency, which is a linchpin of risk mitigation

196 Paech, n 194 above, 433.

197 Settlement Finality Directive, n 143 above, Arts 2(1) and 8; Directive 2001/24/EC of the European Parliament and the Council of 4 April 2001 on the Reorganisation and Winding Up of Credit Institutions, Art 25.

and risk-related regulation. The governance rationale for blockchain-based financial market activity therefore largely corresponds to the axioms of the existing governance framework. Thus, blockchain financial networks need to be subject to a functionally equivalent regulatory and legal framework.

The distributed record, capable of storing complex information such as auto-executable financial transactions, will bring immense efficiency gains to financial markets. The facilitation of financial services brought about by this new type of database will reduce the operational burden and hence decrease reliance on intermediaries and infrastructures. At the same time, the use of distributed databases does not *per se* pose any insurmountable problems in terms of regulation or private law.

However, other features of the original, Bitcoin-inspired, model of blockchain-based networks are unsuitable for use in financial markets from the point of view of effective governance. This is because existing regulatory strategies and legal concepts are largely ineffective if applied to applications that replicate the characteristics introduced by Bitcoin. First, many highly complex regulatory and legal functions in the market are at present taken care of on a small scale, fundamentally in two-party relationships. That intermediary-client approach, one of the cornerstones of regulation, is certainly inefficient to some degree, and a distributed, all-encompassing database may be more efficient and less costly. However, it would seem that some complex governance questions can actually be better referred to a bilateral relationship, as financial services will always remain connected to individual circumstances: for example, anti-money-laundering compliance is necessarily an individual process. Furthermore, the private law that applies to individual clients will generally be a local law, no matter what law applies within the networks through which transactions are administered. Hence, some forms of two-party relationship and, therefore, a certain layer of intermediation, will persist even if the market moved to a blockchain-based setup.

Secondly, there is no *ex post* judgment within Bitcoin-like networks regarding the enforceability of rights arising in these networks. This would make financial networks incompatible with basic societal perspectives. It is true that unstoppable, irreversible self-execution provides more certainty and lowers cost; however, it also entails a total loss of elasticity of behaviour. Elasticity can have its positive sides and is always coupled with institutional and personal responsibility; therefore certainty of execution is not an absolute argument. More importantly, an environment consisting of self-executing contracts and irreversible, computer-induced transactions lacks the element of legal and moral responsibility, which is a fundamental building block of our social order, depriving society from one of its means to implement its policy goals, including insolvency distribution and other rules that protect the interests of third parties and the market as a whole.

In other words, elasticity in decision-making and the existence of *ex post* judgment are the necessary flipside of a system that is to some degree uncertain and inefficient, such as that currently in place. A perfect system could do without judgment, elasticity and responsibility and rely instead on strict, self-enforcing, immutable rules. However, a perfect system would consist, first, of a one hundred per cent fail-safe blockchain network (which cannot exist), which, secondly, administered the assets of *all* parties so that there would no third parties left to be adversely affected. Otherwise, the risk of failure is merely shifted to non-adjusting parties which are those not using the blockchain network, a group which experience shows may consist mainly of non-financial creditors and society as a whole. Some may support a development in that direction and see such an all-encompassing blockchain-based 'world computer' as the necessary complement to the Internet of Things and the algorithmic enhancement of our life experiences.[198] However, such a leviathan is conceptually impossible, as there will always be interests outside the network that general laws and social norms need to protect, quite apart from the consideration that it would by no means be a desirable development.

The good news is that the financial industry does not plan to dispose of these elements entirely. There is a general understanding that blockchain-based financial networks should operate within the reach of law, courts and supervisors. So far, however, the potential negative externalities of increased certainty inside the network on the world outside have not been sufficiently acknowledged. Yet such recognition is the prerequisite for the regulatory and legal integration of blockchain-based financial services. It mainly entails setting boundaries on the blockchain characteristics of immutability and unstoppable execution.

As a result, the expected blockchain revolution will primarily be a technological one, introducing new ways of transaction processing, recording and reporting that will render the financial market significantly more efficient. As far as the governance of blockchain networks is concerned, the current strategies will remain largely the same. Accordingly, state-remote networks, ie networks similar to Bitcoin or Ethereum, cannot serve as models for blockchain financial networks. By contrast, governments would be well advised to cooperate in creating a supportive governance framework for regulated networks to ensure that blockchain technology can be used for the benefit of the market as a whole.

198 See Ethereum, 'Ethereum: The World Computer' (video) at https://www.youtube.com/watch?v=j23HnORQXvs.