THE DISTRIBUTED LIABILITY OF DISTRIBUTED LEDGERS: LEGAL RISKS OF BLOCKCHAIN

*Dirk A. Zetzsche**
*Ross P. Buckley***
*Douglas W. Arner****

The transformative potential of distributed ledger technology ("DLT"), especially in the financial sector, is attracting enormous interest. Many financial institutions are investing heavily in proof-of-concept demonstrations and the rollout of pilot applications of DLT technology. Part of the attraction of distributed ledger systems such as Blockchain lies in transcending law and regulation. From a technological perspective, DLT is generally seen as offering unbreakable security, immutability, and unparalleled transparency, making law and regulation unnecessary. Yet while the law may be dull and the technology exciting, the impact of the law cannot be simply wished away. With data distributed among many ledgers, legal risk remains. DLT projects may well be found by courts to constitute joint ventures, with liability spread across all owners and operators of systems serving as distributed ledgers. Instead of being subject to law nowhere, organizers may instead be subject to the law wherever there are system users. Regulators seeking to support appropriate approaches

* Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Faculty of Law, Economics and Finance, University of Luxembourg, and Director, Centre for Business and Corporate Law, Heinrich-Heine-University, Düsseldorf, Germany.

** Scientia Professor, KPMG Law – King & Wood Mallesons Professor of Innovative Disruption, and Member, Centre for Law, Markets and Regulation, UNSW Sydney.

*** Kerry Holdings Professor in Law, University of Hong Kong.

The authors gratefully acknowledge the financial support of the following: the Luxembourg National Research Fund, project "A New Lane for Fintechs—SMART Regulation," INTER/MOBILITY/16/11406511; the Australian Research Council, project "Regulating a Revolution: A New Regulatory Model for Digital Finance"; and the Hong Kong Research Grants Council Theme-Based Research Scheme, project "Enhancing Hong Kong's Future as a Leading International Financial Centre"; and the research assistance of Katharine Kemp, Jessica Chapman, Tsany Ratna Dewi, Paul Friedrich, and Cheng-Yun Tsang.

The authors are grateful for comments and remarks provided by Michael Aaron, Jànos Barberis, Iris Barsan, Isabelle Corbisiere, Scott Farrell, Holger Fleischer, Annabel Griffin, Rob Hanson, Katja Langenbucher, Alain Pietrancosta, Gerald Spindler, Erik P.M. Vermeulen, Markus Willms, as well as participants at conferences and workshops organized by IJRS Sorbonne–Paris I, the Max Planck Institute for Comparative and International Private Law, Humboldt University Berlin, Tilburg University, and University of Luxembourg. All responsibility is the authors'.

to twenty-first century financial infrastructure must focus on these legal consequences.

KEYWORDS: Bitcoin, Blockchain, Distributed Ledger Technology, Financial Infrastructure, FinTech, RegTech.

TABLE OF CONTENTS

I. INTRODUCTION

Over the past several years, interest in distributed ledger technology ("DLT") such as Blockchain has exploded.[1] Regulators,[2] consultants,[3] technology firms,[4] and academics[5] are promoting DLT for financial services, among many other potential applications. Blockchain technology has moved beyond

1. Focusing on legal and governance issues only: Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 CONSUMER FIN. L.Q. REP. 232, 232 (2016); Wessel Reijers, Fiachra O'Brolcháin & Paul Haynes, *Governance in Blockchain Technologies & Social Contract Theories*, 1 LEDGER 134, 134 (2016); Trevor I. Kiviat, Note, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 573–75 (2015); Carla L. Reyes, Note, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191, 191–92 (2016); Lewis Rinaudo Cohen & David Contreiras Tyler, *Blockchain's Three Capital Markets Innovations Explained*, INT'L FIN. L. REV. (July 11, 2016), http://www.iflr.com/Article/3563116/Blockchains-three-capital-markets-innovations-explained.html. From the French Literature: Primavera De Filippi & Michel Reymond, *La Blockchain: Comment Réguler sans Autorité*, *in* NUMÉRIQUE: REPRENDRE LE CONTRÔLE 83 (Tristan Nitot & Nina Cercy eds., 2016); Pierre-Marie Lore, *Blockchain: Évolution ou Révolution pour les Contrats en France?*, INSTITUT LÉONARD DE VINCI (2016), http://www.ilv.fr/les-blockchains-sont-elles-des-technologies-adaptees-pour-gerer-les-contrats (analyzing vulnerabilities from a contractual perspective); André Ribeiro, *La Blockchain et wes Potentielles Applications* 40 (2016) (unpublished B.A. thesis) (available at http://archive-ouverte.unige.ch/unige:89544). From the Chinese literature: THE LAW SOC'Y OF HONG KONG, INNOVATIVE APPLICATION OF LAW TO FACILITATE DLT 74 (2017) [hereinafter LAW SOC'Y OF H.K.].

2. IOSCO RESEARCH REPORT ON FINANCIAL TECHNOLOGIES (FINTECH) 47–64 (2017), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf; EUR. SEC. MKTS. AUTH., REPORT: THE DISTRIBUTED LEDGER TECHNOLOGY APPLIED TO SECURITIES MARKETS 2 (2017); *15-311 MR ASIC Publishes Results of New Reviews of High-Frequency Trading and Dark Liquidity*, AUSTL. SEC. INVS. COMMISSION (Oct. 26, 2015), http://asic.gov.au/about-asic/media-centre/find-a-media-release/2015-releases/15-311mr-asic-publishes-results-of-new-reviews-of-high-frequency-trading-and-dark-liquidity.

3. It has been estimated that "distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between $15–20 billion per annum by 2022." *See* SANTANDER INNOVENTURES, OLIVER WYMAN & ANTHEMIS GROUP, THE FINTECH 2.0 PAPER: REBOOTING FINANCIAL SERVICES 15 (2015), http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf; WORLD ECON. FORUM, THE FUTURE OF FINANCIAL INFRA-
STRUCTURE: AN AMBITIOUS LOOK AT HOW BLOCKCHAIN CAN RESHAPE FINANCIAL SERVICES 18 (2016), www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf [hereinafter THE FUTURE OF FINANCIAL INFRASTRUCTURE].

4. *See IBM Blockchain*, IBM, https://www.ibm.com/blockchain (last visited May 16, 2018).

5. Eva Micheler & Luke von der Heyde, *Holding, Clearing and Settling Securities Through Blockchain/Distributed Ledger Technology: Creating an Efficient System by Empowering Investors*, 11 BUTTERWORTHS J. INT'L BANKING & FIN. L. 652, 653 (2016); Philipp Paech, *Securities, Intermediation and the Blockchain: An Inevitable Choice Between Liquidity and Legal Certainty?*, 21 UNIFORM L. REV. 612 (2016); Quinn DuPont & Bill Maurer, *Ledgers and Law in the Blockchain*, KING'S REV. (June 23, 2015), http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/.

cryptocurrencies[6] like Bitcoin,[7] and its application is now being considered for all parts of the financial system. Capital raising,[8] trading,[9] clearing and settlement,[10] global payments,[11] deposits and lending,[12] property and casualty claims processing (InsurTech),[13] digital identity management and authentication,[14] and

6. *See* Edward D. Baker, *Trustless Property Systems and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange*, 45 SW. L. REV. 351, 370 (2015); V. Gerard Comizio, *Virtual Currencies: Growing Regulatory Framework and Challenges in the Emerging FinTech Ecosystem*, 21 N.C. BANKING INST. 131, 133 (2017); Matthew P. Ponsford, *A Comparative Analysis of Bitcoin and Other Decentralised Virtual Currencies: Legal Regulation in the People's Republic of China, Canada, and the United States*, 9 HONG KONG J.L. STUD. 29 (2015). From Spain: Mª Nieves Pacheco Jiménez, *Criptodivisas: Del Bitcoin al MUFG. El Potencial de la Tecnología Blockchain*, 19 REVISTA CESCO DE DERECHO DE CONSUMO 6 (2016).

7. *See* Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*, 17 NEV. L.J. 139, 140–55 (2016); Primavera De Filippi, *Bitcoin: A Regulatory Nightmare to a Libertarian Dream*, 3 INTERNET POL'Y REV. 1, 1 (2014); Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 113 (2012); EDWARD V. MURPHY, M. MAUREEN MURPHY & MICHAEL V. SEITZINGER, BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES (2015), https://fas.org/sgp/crs/misc/R43339.pdf; Nicholas A. Plassaras, *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*, 14 CHI. J. INT'L. L. 377, 379 (2013); Peter Twomey, *Halting a Shift in the Paradigm: The Need for Bitcoin Regulation*, 16 TRINITY C. L. REV. 67, 67 (2013); Joshua J. Doguet, Note, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119, 1119 (2013); Reuben Grinberg, Note, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 171 (2012); Misha Tsukerman, Note, *The Block Is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future*, 30 BERKELEY TECH. L.J. 1127, 1127 (2015); John O. McGinnis & Kyle Roche, *Bitcoin: Order Without Law in the Digital Age* 4 (Nw. Pub. L. Res. Paper No. 17-06, 2017), https://ssrn.com/abstract=2929133. From Germany: Nico Kuhlmann, *Bitcoins—Funktionsweise und Rechtliche Einordnung der Digitalen Währung*, COMPUTER & RECHT 691 (2014); Benjamin Beck & Dominik König, *Bitcoins als Gegenstand von Sekundären Leistungspflichten*, 215 ARCHIV FÜR DIE CIVILISTISCHE PRAXIS 655 (2015); DANIEL KERSCHER, BITCOIN – FUNKTIONSWEISE, CHANCEN UND RISIKEN DER DIGITALEN WÄHRUNG 120 (2d ed., 2013); GERALD SPINDLER & MARTIN BILLE, RECHTSPROBLEME VON BITCOINS ALS VIRTUELLE WÄHRUNG 1357 (2014); FRANZISKA BOEHM & PAULINA PESCH, BITCOINS: RECHTLICHE HERAUSFORDERUNGEN EINER VIRTUELLEN WÄHRUNG—EINE ERSTE JURISTISCHE EINORDNUNG MMR 75 (2014).

8. *See* THE FUTURE OF FINANCIAL INFRASTRUCTURE, *supra* note 3, at 83–91.

9. *See* DAVID SHRIER ET AL., BLOCKCHAIN & TRANSACTIONS, MARKETS AND MARKETPLACES (2016), https://cdn.www.getsmarter.com/career-advice/wp-content/uploads/2017/07/mit_blockchain_transactions_report.pdf; Benito Arruñada, *Blockchain's Struggle to Deliver Impersonal Exchange*, 19 MINN. J.L. SCI. & TECH. 55, 57 (2018); Gareth W. Peters & Guy R. Vishnia, *Blockchain Architectures for Electronic Exchange Reporting Requirements: EMIR, Dodd Frank, MiFID I/II, MiFIR, REMIT, Reg and T2S*, *in* HANDBOOK OF BLOCKCHAIN, DIGITAL FINANCE, AND INCLUSION (David Lee Kuo Chuen & Robert H. Deng eds., 2018).

10. *See* THE FUTURE OF FINANCIAL INFRASTRUCTURE, *supra* note 3, at 119–27; Micheler & von der Heyde, *supra* note 5; Paech, *supra* note 5, at 612–639. Blockchain-based company Ripple operates almost like an interbank clearing service. Ripple was fined by the U.S. Department of Treasury for functioning as an unlicensed money transmitter. *See* Joseph B. Evans, *Bitcoin, Money and Funds: The Application of the Unlicensed Money Transmitting Services Statute to Virtual Currency*, FORDHAM J. CORP. & FIN. L. (Nov. 14, 2016), https://news.law.fordham.edu/jcfl/2016/11/14/bitcoin-money-and-funds-the-application-of-the-unlicensed-money-transmitting-services-statute-to-virtual-currency.

11. *See* Harry Leinonen, *Decentralised Blockchained and Centralised Real-Time Payment Ledgers: Development Trends and Basic Requirements*, *in* TRANSFORMING PAYMENT SYSTEMS IN EUROPE 236 (Jakub Górka ed., 2016); THE FUTURE OF FINANCIAL INFRASTRUCTURE, *supra* note 3, at 21, 39, 46–55.

12. *See* THE FUTURE OF FINANCIAL INFRASTRUCTURE, *supra* note 3, at 65–82, 110–18 (exploring the potential of Bitcoin for syndicated loans and trade finance as well as asset rehypothecation).

13. *See* THE FUTURE OF FINANCIAL INFRASTRUCTURE, *supra* note 3, at 40, 56–64.

RegTech solutions[15] (such as automated compliance, administration and risk management, and anti-money laundering and client suitability checks) have all been identified as significant potential DLT use cases and as areas that will benefit from the advantages DLT offers. In many recent instances, use cases have now moved through the proof-of-concept stage to the pilot stage.

At the same time, legal concerns are emerging. The discussion so far has focused on: investment fraud;[16] the classification of cryptocurrencies as securi

14. *See* WORLD ECONOMIC FORUM, A BLUEPRINT FOR DIGITAL IDENTITY: THE ROLE OF FINANCIAL INSTITUTIONS IN BUILDING DIGITAL IDENTITY 60 (2016), http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf (stressing the need for a more secure digital identity system, relying on Bitcoin characteristics) [hereinafter A BLUEPRINT FOR DIGITAL IDENTITY]; THE FUTURE OF FINANCIAL INFRASTRUCTURE, *supra* note 3, at 22; STEWART BOND, IT WAS ONLY A MATTER OF TIME—DIGITAL IDENTITY ON BLOCKCHAIN (2017). For particular discussion on IBM's "Identity Management with Blockchain," see *IBM Blockchain*, *supra* note 4, at 1.

15. *See* THE FUTURE OF FINANCIAL INFRASTRUCTURE, *supra* note 3, at 92–109 (exploring the potential of Bitcoin automated compliance and proxy voting). On RegTech, generally, see Douglas W. Arner, Jànos Barberis & Ross P. Buckley, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, NW. J. INT'L L. & BUS. 371, 373 (2017).

16. Kiviat, *supra* note 1, at 569; Derek A. Dion, Note, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash*, 2013 U. ILL. J.L. TECH. & POL'Y 165, 167.

ties, derivatives, commodities, currency or other assets;[17] systemic risk regulation; central bank functions;[18] money laundering;[19] and taxation.[20] We seek to add another, private-law dimension that has received little attention.[21]

In analyzing legal and regulatory issues around DLT, the starting point is to identify the central characteristics of the technology and analyze these within existing legal and regulatory frameworks. In this foundational analysis, legal

17. Jerry Brito, Houman Shadab & Andrea Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144, 155–205 (2014); Ed Howden, Comment, *The Crypto-Currency Conundrum: Regulating an Uncertain Future*, 29 EMORY INT'L L. REV. 741, 761–69 (2015); Ponsford, *supra* note 6, at 29; Kiviat, *supra* note 1, at 594–95; Reyes, *supra* note 1, at 213–22 (summarizing U.S. academic approaches categorizing DLT); Tsukerman, *supra* note 7, at 1153–56; Philipp Paech, *The Governance of Blockchain Financial Networks*, MODERN L. REV. 1073, 1074–75 (2017); Gareth W. Peters, Efstathios Panayi & Ariane Chapelle, *Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective*, J. FIN. PERSPECTIVES, Winter 2015, at 92; McGinnis & Roche, *supra* note 7, at 53–58; Andrew Hinkes, *The Law of the DAO*, COINDESK (May 19, 2016), http://www.coindesk.com/the-law-of-the-dao (arguing that investment in the DAO is a security for the purpose of US securities regulation); Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, 24 U. MIAMI BUS. L. REV. 1, 10–11 (2016). In a report issued July 25, 2017, the SEC found that the "coins" in one prominent Initial Coin Offering ("ICO"), the DAO, were in fact securities. As discussed in the Report, virtual coins or tokens may be securities and subject to the U.S. federal securities laws. *See* SEC, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Rel. No. 81207 (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

18. Nicholas A. Plassaras, *Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF*, 14 CHI. J. INT'L L. 377, 391 (2013); Twomey, *supra* note 7, at 72; Doguet, *supra* note 7, at 1121–23; Grinberg, *supra* note 7, at 172–73.

19. The notable example being the notorious Silk Road. *See* United States v. Ulbricht, 31 F. Supp. 3d 540, 569 (S.D.N.Y. 2014); United States v. Faiella, 39 F. Supp. 3d 544, 546 (S.D.N.Y. 2014); Baker, *supra* note 6, at 371–74; Comizio, *supra* note 6, at 135–38, 141–46, 162; LAW SOC'Y OF H.K., *supra* note 1, at 98; Tsukerman, *supra* note 7, at 1147–59, 1166–67; Max I. Raskin, Note, *Realm of the Coin: Bitcoin and Civil Procedure*, 20 FORDHAM J. CORP. & FIN. L. 970, 980–83 (2015).

20. *Cf.* Treasury Inspector General for Tax Administration, *As the Use of Virtual Currencies in Taxable Transactions Becomes More Common, Additional Actions Are Needed to Ensure Taxpayer Compliance*, Ref No. 2016-30-083, 1–2 (Sept. 21, 2016), https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf; Nika Antonikova, Paper, *Real Taxes on Virtual Currencies: What Does the I.R.S. Say?*, 34 VA. TAX REV. 433, 433 (2015); Erin M. Hawley & Joseph J. Colangelo, *Bitcoin Taxation: Recommendations to Improve the Understanding and Treatment of Virtual Currency*, ENGAGE, July 2014, at 4 (2014); Sarah Gruber, Note, *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?*, 32 QUINNIPIAC L. REV. 135, 141–50 (2013); Tsukerman, *supra* note 7, at 1150–52, 1159–61. From a German perspective: BOEHM & PESCH, *supra* note 7 (mentioning extraordinary reliance on Bitcoin in the vicinity of Cyprus mandatory tax levies on deposits). *See generally* KIM-PATRICK ECKERT, STEUERLICHE BETRACHTUNG ELEKTRONISCHER ZAHLUNGSMITTEL AM BEISPIEL SOG. BITCOIN-GESCHÄFTE, 38 DB 2108 (2013).

21. *Cf.* the underweighted common law dimension of distributed ledgers: Shawn Bayern, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 WASH. & LEE REV. ONLINE 22 (2014); Paech, *supra* note 17, at 23–34; Raskin, *supra* note 19, at 972–74. From a German civil law perspective: Beck & König, *supra* note 7. Very little attention has been paid to the private law sphere in French regulation, and the only legality mandate issued by French regulators dealt with AML and taxation issues. *But see* Press Release, Michel Sapin, Ministre des Finances et des Comptes Publics, Réguler les Monnaies Virtuelles (July 11, 2014) (available at http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/17768.pdf) ("Limiter l'anonymat en imposant une prise d'identité lors de l'ouverture par un professionnel d'un compte en monnaies virtuelles pour un tiers, et en imposant une vérification d'identité pour les retraits et dépôts aux 'distributeurs' de bitcoin." – transl. "To limit anonymity by imposing on professionals a duty of establishing identity when opening a virtual currency account for a third party, and by imposing on Bitcoin 'distributors' a duty of verification of identity in case of withdrawal.").

and regulatory issues must be considered in the specific context of individual use cases, proofs-of-concept, and pilots. Of central importance is the potential of DLT as a trust solution.[22] The trust-enhancing function of multiple ("distributed") entities together providing authentication rather than one "centralized" ledger is claimed to lead to (1) disintermediation of traditional intermediaries and clearing and settlement systems (resulting in greater security and transparency), (2) enhanced efficiency and speed, (3) lower transaction costs, and (4) enhanced market access.

This Article focuses upon the *potential liability of DLT participants*. This is because legal liability (if any) will simply not disappear with DLT, although it is often (from our perspective, over-enthusiastically[23]) wished away by those who promote and analyze the technology[24] or praise its economic potential.[25] This matters, as distributed ledgers are often hailed as the answer to ever-increasing cybersecurity risks. While distributed ledgers may well be more secure than traditional centralized ledgers, recent events call for an analysis of who will bear DLT losses and responsibility for damages in connection with a blockchain. Some notable events[26] include the following:

- A hack from 2011 until February 2014 resulted in losses of 750,000 customer Bitcoins and 100,000 Bitcoins owned by the Japanese Bitcoin exchange, Mt. Gox, then the largest Bitcoin exchange in the world. The leading explanation called this a malleability attack relying on a hot-wallet

22. *See* Michael Crosby et al., *BlockChain Technology: Beyond Bitcoin*, 2 APPLIED INNOVATION REV. 6, 9 (2016).

23. *See* Massimo Morini, *From "Blockchain Hype" to a Real Business Case for Financial Markets*, 45 J. FIN. TRANSFORMATION 30, 33 (2017).

24. *Cf.* Mélanie Dulong de Rosnay, *Responsabilité*, *in* ABÉCÉDAIRE DES ARCHITECTURES DISTRIBUÉES 203–04 (Cécile Méadel & Francesca Musiani eds., 2015) (stating, without in-depth legal analysis, that distributed networks would be neither property, nor contract, nor otherwise legally governed); Mélanie Dulong de Rosnay, *Peer-to-Peer as a Design Principle for Law: Distribute the Law*, J. PEER PROD. (Jan. 2015), http://peerproduction.net/issues/issue-6-disruption-and-the-law/peer-reviewed-articles/peer-to-peer-as-a-design-principle-for-law-distribute-the-law (last visited May 16, 2018) [hereinafter Dulong de Rosnay, *Peer-to-Peer*] (taking the position that law focuses on individual rights and arguing in favor of an expansion and adaptation of law to assign rights and obligations to communities rather than individuals). *But see* Paech, *supra* note 17, at 23–24, 28 (stating that system issues render enforcement difficult, implying that legal claims are granted by the law, and demanding that "de facto acquisition on the basis of the operation of software needs to be recognised by private law itself"–without further details).

25. Alistair Milne, Cryptocurrencies from an Austrian Perspective (May 18, 2017) (unpublished manuscript) (available at https://ssrn.com/abstract=2946160).

26. *See also* MURPHY, MURPHY & SEITZINGER, *supra* note 7, at 8–9 (citing an additional five "smaller" liability events in 2012 and 2013, including Bitcoin Savings and Trust's insolvency (US$5.6 million in damages), the hacks of Bitfloor (US$250,000), Instawallet (US$4.6 million), Australian Bitcoin Bank (more than US$1 million), and Bitcoin Foundation).

bug.[27] Mt. Gox subsequently declared bankruptcy, citing losses from the hack amounting to $473 million (USD) at the time of filing.[28]

- In January 2015, Luxembourg- and London-based Bitstamp, the second largest Bitcoin exchange by 2016 in terms of volume traded, suffered from a hot-wallet hack leading to the loss of 19,000 Bitcoins, valued at about $5.1 million (USD). Bitstamp subsequently suspended services for nearly a week during which client deposits were not accessible.[29]
- In 2016, $53 million (USD) of the over $150 million (USD) crowd-funded assets in DLT-based virtual currency Ether—held in the investor-directed, DLT-enabled Decentralized Autonomous Organization ("DAO")[30]—were channeled to a third-party-controlled account after exploiting previously published vulnerabilities[31] in the DAO code.[32] A White Hat or Robin Hood counter attack led to most of the lost Ether being recaptured.[33]
- In 2016, Hong Kong-based Bitfinex, one of the world's largest bitcoin exchanges, lost 119,756 Bitcoins, with a market value at the time of between $66 and $72 million (USD), in a hack that involved its multi-signature accounts.[34] Bitfinex decided to apportion losses from the theft across the company's clients and assets, widening the group of those affected by the

27. Doubts persist as to the technical reason for this loss. The fact that 200,000 Bitcoin were later found on a discarded hard drive was troubling. *See The Troubling Holes in Mt. Gox's Account of How It Lost $600 Million in Bitcoins*, TECH. REV. (Apr. 4, 2014), https://www.technologyreview.com/s/526161/the-troubling-holes-in-mtgoxs-account-of-how-it-lost-600-million-in-bitcoins.

28. *See* Daniel Cawrey, *Mt. Gox Trading Halts as Bitcoin Businesses Move to Assure Investors*, COINDESK (Feb. 25, 2014, 5:12 PM), http://www.coindesk.com/mt-gox-trading-halts-bitcoin-businesses-move-assure-investors; Brendan Conway, *Mt. Gox Bitcoin Exchange Files for Bankruptcy Protections*, BARRON'S (Feb. 28, 2014, 8:35 AM), https://barrons.com/articles/mt-gox-bitcoin-exchange-files-for-bankruptcy-protection-1393594521; Comizio, *supra* note 6, at 138–40; Tsukerman, *supra* note 7, at 1150.

29. Mariella Moon, *Bitcoin Exchange Loses $5 Million in Security Breach*, ENGADGET (Jan. 6, 2015), http://www.engadget.com/2015/01/06/bitstamp-bitcoin-exchange-hack.

30. The DAO is associated with a Swiss company, but its main actors are German. For an overview of the DAO's architecture, see Dino Mark, Vlad Zamfir & Emin Gün Sirer, *A Call for a Temporary Moratorium on "The DAO,"* HACKING DISTRIBUTED (May 27, 2016, 1:35 PM), http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium; Mary-Ann Russon, *The Curious Tale of Ethereum: How a Hacker Stole $53m in Digital Currency and Could Legally Keep It*, INT'L BUS. TIMES (June 20, 2016, 6:28 PM), https://www.ibtimes.co.uk/curious-tale-ethereum-how-hacker-stole-53m-digital-currency-could-legally-keep-it-1566524; Russell Brandom, *How an Experimental Cryptocurrency Lost (and Found) $53 Million*, VERGE (June 17, 2016, 3:11 PM), https://www.theverge.com/2016/6/17/11965192/ethereum-theft-dao-cryptocurrency-million-stolen-bitcoin.

31. *See* Russon, *supra* note 30.

32. *See* Brandom, *supra* note 30.

33. For further details, see Quinn DuPont, *Experiments in Algorithmic Governance: An Ethnography of "The DAO," a Failed Decentralized Autonomous Organization*, *in* BITCOIN AND BEYOND: CRYPTOCURRENCIES, BLOCKCHAINS, AND GLOBAL GOVERNANCE 2 (Malcolm Campbell-Verduyn ed., 2017).

34. Stan Higgins, *The Bitfinex Bitcoin Hack: What We Know (and Don't Know)*, COINDESK (Aug. 5, 2016, 5:44 PM), http://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know.

losses beyond those holding the multi-signature accounts that were hacked. Accordingly, *all* Bitfinex clients lost a significant 36% of their holdings.[35]

- On July 19, 2017, attackers stole $32 million (USD) worth of Ether, by exploiting a vulnerability in the multi-signature wallets of a popular Ethereum client called Parity. The attack prompted a volunteer group of coders calling themselves the "White Hat Group" to take it upon themselves to "rescue" $208 million (USD) from the other 500 vulnerable wallets before the attackers could get a hold of them. The White Hat Group breached the wallets using the same vulnerability as the attackers and funneled the funds into the group's own account, apparently "running afoul of federal laws on criminal hacking."[36]

As these examples show, *risk does not vanish if financial services are provided via distributed ledgers*. With DLT, the data and the risks, formerly concentrated in a centralized ledger, are distributed across all participants ("nodes").

The analysis in this Article of the liabilities associated with DLT should serve regulators, globally, who are currently working to identify risks likely to arise from DLT, as well as market participants involved in DLT systems. In particular, the International Organization of Securities Commissions ("IOSCO") is reported to be "working to identify risks to business models from digital disruption like the blockchain,"[37] with European regulator ESMA (the European Securities and Markets Authority)[38] and other IOSCO members entering into large-scale fact gathering and analysis. In a similar vein, the Financial Stability Board has started to look into risks and vulnerabilities created by Blockchain.[39]

Part II of this Article considers the move from concentrated to distributed ledgers and analyzes the underlying features of DLT that make it so potentially attractive to financial services—in particular, its security—and its related characteristics of transparency and immutability.

Part III reveals that joint control is the preeminent feature of distributed ledgers, regardless of whether the system is permissioned or permissionless. Part III also outlines the legal consequences of joint control, demonstrating that

35. *All Bitfinex Clients to Share 36% Loss of Assets Following Exchange Hack*, GUARDIAN (Aug. 8, 2016, 2:29 PM), https://www.theguardian.com/technology/2016/aug/07/bitfinex-exchange-customers-receive-36-percent-loss-tokens.

36. Jordan Pearson, *How Coders Hacked Back to 'Rescue' $208 Million in Ethereum*, VICE (July 24, 2017, 4:21 PM), https://motherboard.vice.com/en_us/article/qvp5b3/how-ethereum-coders-hacked-back-to-rescue-dollar208-million-in-ethereum.

37. *Thinking Forward*, MARKETVOICE (Jan. 19, 2016), https://marketvoice.fia.org/issues/2016-01/thinking-forward; *see also* EUR. SEC. MKTS. AUTH., *supra* note 2, at 8.

38. *See* EUR. SEC. MKTS. AUTH., *supra* note 2, at 3.

39. *See* Press Release, Financial Stability Board, Meeting of the Financial Stability Board in Tokyo on 30–31 March (Mar. 31, 2016) (available at http://www.fsb.org/2016/03/meeting-of-the-financial-stability-board-in-tokyo-on-30-31-march) ("The Plenary reviewed major areas of financial technology innovation, including distributed ledger technology, and proposed a framework for categorising them and assessing any financial stability implications. Plenary members discussed the issues raised for public authorities by these technologies, possible steps to address potential risks, and opportunities for cooperation in the FSB and with the standard-setting bodies to deepen analysis and develop regulatory perspectives.").

regardless of whether it is considered from the standpoint of the law of torts, contracts, or partnership/company law, joint control potentially results in joint liability. We further show that joint control impacts the legal consequences of the three most likely risk sources in a blockchain which include (1) failures at the level of the node, (2) failures at the level of client/user, and (3) unintended third-party access (cyberattack).

Part IV ponders the consequences for regulated intermediaries and regulatory systems that seek to participate in distributed ledger systems. Financial institutions need to carefully consider the legal design of any such system. If a distributed ledger links multiple legal entities, all entities in the system need to consider contingent liability risk, including putting risk and compliance management systems in place and holding appropriate levels of risk capital (or providing for meaningful insurance coverage). While some may believe that, from a technology perspective, distributed ledgers may be difficult to set up[40] and easier to handle long-term, from a legal perspective the opposite may be true: they are easy to set up but come with ongoing, long-term legal consequences. From a pure risk perspective, concentrating precautionary measures and liability in one entity (a joint venture) that holds the legal title in multiple ledgers could turn out to be the best solution. While this concentrated design works well among the subsidiaries of one financial conglomerate, it is doubtful that independent financial institutions will be willing to give up control over their clients' data in this way.

Part V concludes by considering these options.

II. FEATURES OF DISTRIBUTED LEDGER TECHNOLOGY

A. The Ledger Concept

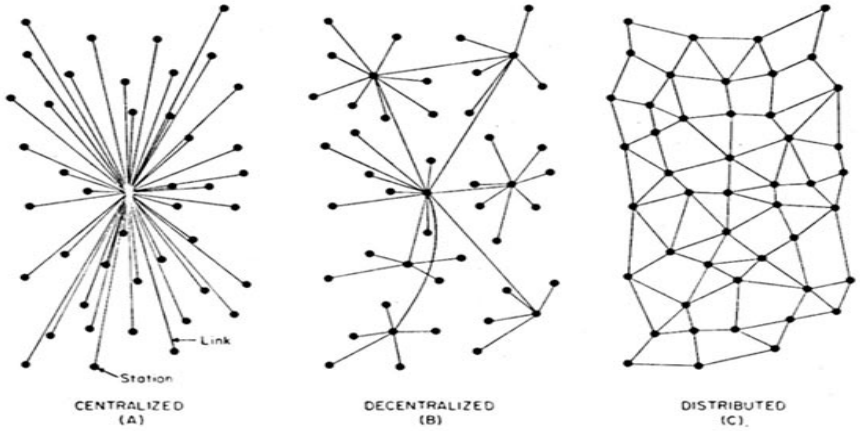
The modus operandi of distributed ledgers is best understood by looking at their counterpart, the centralized ledger. Centralized ledgers are the most common data storage device in finance today.[41] In a centralized ledger, data are stored on the ledger, and the trusted administrator of the ledger maintains it, recording transfers of assets and the like upon receipt of appropriately verified

40. While traditional setup takes time, effort and resources, Blockchain-as-a-Service ("BAAS") providers such as IBM ("IBM Blockchain"), Microsoft ("Azure") and Intel enable the setup of a full-meshed network in just a few hours or even less. *See, e.g.*, Toshendra Sharma, *Setting up Ethereum Blockchain on Microsoft Azure in 1 Hour*, https://www.udemy.com/setting-up-ethereum-blockchain-on-microsoft-azure-in-1-hour (last visited May 16, 2018); *Blockchain 101 Infographic: Understand What Blockchain Is, How It Works, and the Key Benefits to Enterprises*, IBM: BLOCKCHAIN, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=
XI912346USEN (last visited May 16, 2018); Blair Hanley Frank, *Microsoft Launches Super-Speedy Clouds Networking Out of Beta*, VENTUREBEAT (Jan. 5, 2018, 3:12 PM), https://venturebeat.com/2018/01/05/microsoft-launches-super-speedy-cloud-networking-out-of-beta; *Intel Blockchain Technology Offered as a Service in Oracle Cloud*, INTEL: NEWSROOM (Oct. 2, 2017), https://newsroom.intel.com/news/intel-blockchain-technology-offered-service-oracle-cloud.

41. Shyam Sankar, *Centralized Ledgers vs. Distributed Ledgers (Layman Understanding)*, MEDIUM (July 12, 2017), https://medium.com/@shyamshankar/centralized-ledgers-vs-distributed-ledgers-layman-understanding-52449264ae23.

notifications. Risks exist. The ledger could be destroyed, or more likely, hacked or otherwise compromised so that the original data are held for ransom or manipulated and replaced by new, inaccurate data. Mathematical approaches can be used to define how much effort is necessary to manipulate any given server. As such, every single server *can* be manipulated with sufficient computing power.[42]

FIGURE 1[43]



Distributed ledgers address these problems by raising the barriers for manipulation of stored data. Rather than relying on the hub-and-spokes model of centralized ledgers, or the hubs and spokes of decentralized ledgers, in distributed ledgers, many data storage points (nodes) are all connected with each other and store all data simultaneously, together constituting the common ledger. DLT requires consensus of those nodes rather than just the confirmation by one hierarchically structured storage device, as with a centralized ledger. The technical details of how to achieve consensus vary—technology allows, for instance, for proof-of-work concepts[44] or proof-of-stake concepts—and the tech-

42. In theory, any system, including a distributed system, can be brute-forced, trespassing preventive controls. If all else fails, attackers may turn to brute-force attacks, *i.e.*, multiple password guessing. System operators may counter by using detective controls. *See* Dinei Florêncio, Cormac Herley & Baris Coskun, *Do Strong Web Passwords Accomplish Anything?*, USENIX: WORKSHOP ON HOT TOPICS IN SECURITY (2007), https://www.usenix.org/legacy/event/hotsec07/tech/full_papers/florencio/florencio.pdf; Jung-Sik Cho, Sang-Soo Yeo & Sung Kwon Kim, *Securing Against Brute-Force Attack: A Hash-Based RFID Mutual Authentication Protocol Using A Secret Value*, 34 COMPUTER COMM. 391, 391 (2011); Jung-Sik Cho, Young-Sik Jeong & Sang Oh Park, *Consideration on the Brute-Force Attack Cost and Retrieval Cost: A Hash-Based Radio-Frequency Identification (RFID) Tag Mutual Authentication Protocol*, 69 COMPUTERS & MATHEMATICS APPLICATIONS 58, 64 (2015).

43. PAUL BARAN, THE RAND CORP., ON DISTRIBUTED COMMUNICATIONS: I. INTRODUCTION TO DISTRIBUTED COMMUNICATIONS NETWORKS 2 (1964), https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf. Baran's diagram for distributed ledgers is now inaccurate. In modern distributed ledgers, in principle, all nodes can connect and communicate with each other.

44. In a proof-of-work system, multiple servers ("nodes") all try to solve one mathematical problem. Solving the problem requires data processing capacity and energy. The first node to solve the problem is compensated, while all others use the solution provided by the first node to verify that the problem has been cor-

nology adopted defines how the consensus mechanism can be gamed. Regardless, data stored on a distributed ledger are less likely to be manipulated in any given case as compared to data stored on one, equally secure server.

Assume that there are *N* nodes (rather than one centralized ledger) and that *E* describes the effort necessary to break into any single server. Given that all other conditions (security of each server, etc.) are equal,[45] we would expect the efforts necessary to manipulate all servers linked in the ledger to be *N* x *E* rather than 1 x *E*. The number of servers which would need to be manipulated to alter the outcome will depend on the number of servers necessary for consensus and the number of nodes involved. If $N > 1$, the distributed ledger is more secure than the concentrated one.

"Blockchain" refers to how data are stored on the ledger. Rather than being stored individually, data are stored in an encrypted block bundled with other data. The block serves as the container of multiple data points, and all blocks are stored in a specific order (the "chain"). Each block contains a timestamp and a link to the previous block, with each individual block being separately encrypted and built on the basis of previous encrypted blocks. Rather than manipulating one point alone, the bundling of multiple datasets in one block requires a cyberattack to manipulate the whole block of data as well as—due to the time stamp and link—the blocks before and after the attacked block.

B. Permissioned vs. Permissionless DLTs

DLT can take various forms. In particular, DLT systems can be permissioned or permissionless. Permissioned systems are essentially private networks where data authorization depends upon the agreement of multiple predefined servers. Permissioned systems require an organization and governance structure regulating at least who is permitted to participate and usually the basis upon which they may participate. For instance, the DLT-based, peer-to-peer digital payment network Ripple uses a network of trusted parties ("validation" nodes) that constantly compare their transaction records.[46]

rectly solved; thereby, the solution to the mathematical problem assumes the function of a unique, one-time-use code.

45. In practice, nodes of a distributed system do not typically have the same level of security as concentrated systems: (1) a chain is only as strong as its weakest link (most of the times, the endpoint and the human controlling it); (2) even if the DLT as "supra layer" is secure, the "underlying layer" may be less strong, and both pose risks to DLT security; (3) a distributed system is much more difficult to restore than a central system. If a central system is compromised and the date/time can be determined, running the ledger on a backup could effectively counter the hacker attack (as long as the backup has not been compromised). In a distributed system, due to governance issues once compromised, there are no easy ways to restore the data chain. Altogether this undermines DLT security. *See infra* Section III.A.

46. For a brief overview on Ripple's technology, see Vitalik Buterin, *Introducing Ripple: A Detailed Look at Cryptocurrency's New Kid on the Block*, BITCOIN MAG. (Feb. 26, 2013, 9:19 PM), https://bitcoinmagazine.com/articles/introducing-ripple (the technology underlying Ripple is able to integrate established financial intermediaries which may explain Ripple's current success); *see also* Stan Higgins, *Stellar Network Fork Prompts Concerns Over Ripple Consensus Protocol*, COINDESK (Dec. 9, 2014, 8:26 PM), https://www.
coindesk.com/stability-questions-dog-ripple-protocol-stellar-fork (arguing that permissioned blockchains such

In contrast, permissionless blockchains such as Bitcoin operate on public domain software and allow anyone who downloads and runs the software to participate. In some cases, even the code is further developed in the public domain. The participants in those distributed ledgers may not know who else is running a server functioning as a node at any given time. There is an additional security element in the unknown that is inherent in this structure: if the number of overall nodes is known, a cyberattack may be planned with greater certainty given that the maximum number of nodes is certain.[47] If nodes come and go depending on participants, efforts focused on certain nodes may prove fruitless if those nodes have stopped operations or are in excess of the number needed for consensus. The number of nodes required for a consensus is set in the code underlying the system and is thus a fundamental aspect of the design of any system. This also provides one of the major, known vulnerabilities in many blockchain systems, including Bitcoin.

C. Storage Trust Issue Solved

The solution to the storage trust issue leads to efficiency gains wherever storage trust is of the essence. Since most financial intermediation is based on trust—clients give their financial or other resources to someone else—enhancing trust in storage could reduce risk premiums resulting from a lack of trust.

The trust that *the ledger* is maintained and thus the data retrievable (similar to a book copy that is stored in the archives), however, depends on the system's design. All systems face the risk of "invalidity through obsolescence and boredom"[48]: without a community of nodes running the protocol and verifying transactions, the system stops working. If all members have moved to a new system, data stored on the blockchain might become inaccessible. DLTs pay nodes directly or indirectly for running the protocol. For instance, Bitcoin maintains incentives with "mining": "[B]y assigning parts of the ledger to miners who, competing with each other, win the proof-of-work lottery. Incentivization is critical to ensure that miners do not grow bored and stop mining, thereby failing to provide the essential verification mechanism."[49]

D. Examples

There are multiple fields where DLT may have great potential. One of the most widely discussed applications of storage trust relates to *clearing and settlement*.[50] Generally, a central securities depository ("CSD") functions as a cen-

as Ripple might be more vulnerable than permissionless ones); Diana Ngo, *Banks Unite Around Ripple to Launch Blockchain-Based Cross-Border Wiring Service*, COINJOURNAL (Apr. 3, 2017), https://coinjournal.net/banks-unite-around-ripple-launch-new-cross-border-wiring-service.

47. IT experts refer to this strategy as "security through obscurity."

48. DuPont & Maurer, *supra* note 5.

49. *Id.*

50. *Id.*

tralized ledger that records all transactions and changes in ownership. All custodians and depositories are linked to the CSD, and clearing and settlement costs are defined by the CSD's charges.[51] With DLT, the centralized ledger could be replaced by a distributed network of certain core depositories holding together the various securities. This proposition could become more powerful in combination with smart contracts leading to automatic execution.

Another potential use for DLT includes fields where proprietary access to data creates or enhances a dominant position in a market. With DLT, *data access is mutualized*. This may create both opportunities and difficulties. If we envision an AML/KYC ("anti-money laundering" and "know your customer") hub being maintained for a financial center like Hong Kong or Luxembourg, no entity would consent to its competitor holding its client data. A DLT system may enable a compromise in that all entities simultaneously hold all client data and could therefore greatly benefit from scale economies resulting from, for instance, AML/KYC checks needing to be undertaken only once. At the same time, given the sensitivity of data, financial institutions would insist on the most secure technology. DLT could simultaneously address the governance and storage trust issues associated with a centralized AML/KYC hub.[52]

III. DLT AND THE RISKS OF DISTRIBUTED LIABILITY

DLT addresses the storage trust issue. DLT ensures the validity of datasets by spreading data over many nodes which must agree, via the previously determined consensus mechanism, to confirm data validity. DLT can ensure that data are not manipulated during storage better than other technologies.[53] DLT can also ensure that the party making a transfer has title on the ledger to the asset being transferred and is not able to transfer it twice to separate buyers.[54] Beyond these inbuilt protections, however, DLT does not make inaccurate data accurate. Inaccurate data stored via DLT remains inaccurate; the "garbage in, garbage out" dilemma holds.[55]

The important point here is that while DLT may enhance data security, it is not bulletproof. DLT has certain characteristics that could result in undesira-

51. *Frequently Asked Questions*, EUR. CENT. SECS. DEPOSITORIES ASS'N, https://ecsda.eu/facts/faq (last visited May 16, 2018).

52. DLT could be beneficial regardless of which data can be accessed by users of the AML/KYC hub. Access to data may be organized differently than storage. For instance, financial institutions that rely on the client data stored via the ledger may receive only a green/yellow/red light, while their underlying server infrastructure achieves consensus on the data that provide the basis for the AML/KYC assessment.

53. Allison Berke, *How Safe Are Blockchains? It Depends*, HARV. BUS. REV., (Mar. 27, 2017), https://hbr.
org/2017/03/how-safe-are-blockchains-it-depends.

54. Levi Morehouse, *The Technology That Will Change Accounting*, FORBES (June 14, 2017), https://www.forbes.com/sites/forbesfinancecouncil/2017/06/14/the-technology-that-will-change-accounting/#2dd353506916.

55. This facilitates abuse because the dividing line between true and false information is blurred. *See* Gruber, *supra* note 20, at 135 (citing the case where an anonymous person threatened to disclose former presidential candidate Mitt Romney's tax returns unless he was paid a certain amount; it was uncertain whether the tax data was accurate).

ble data distribution, data loss, or data manipulation. All of these lead to questions about responsibility and liability, issues considered in this Section.

A. Liability Risks Associated with DLT

DLT commonly gives rise to at least three major types of potential liability risk: ledger transparency risks, cyber risks, and operational risks.

1. Risks from Increased Ledger Transparency

DLT stores data by spreading them over multiple nodes. Every node operator has access to the data stored on the ledger.[56] While a certain level of transparency is a precondition for the enhanced level of trust that DLT creates, the enhanced level of transparency could enable repersonalization of data stored on the distributed ledger or enable nodes to make an informed guess as to identities entering into certain transactions. While data can be encrypted before being stored on a blockchain, rendering it effectively unreadable to third persons, metadata is necessarily public. Two main legal risks derive from this enhanced level of transparency, one relating to data privacy and another to insider trading and market abuse.

a. Violation of Data Privacy

The transparency characteristics of distributed ledgers and data privacy are in tension. For instance, Bitcoin reveals considerable information about users' profiles, enabling repersonalization of pseudonymous data.[57] Indeed,

56. For instance, in Bitcoin, all the data are on the blockchain except the identities of the owners. To know that, one requires the private key. The private key is stored on the owner's wallet rather than the ledger. "However, anyone can see who owns each block, via its public header information, and can follow the links through the entire chain right back to the first block." *Cf.* Jude Umeh, *Blockchain Double Bubble or Double Trouble?*, ITNOW, Spring 2016, at 58.

57. Elli Androulaki et al., *Evaluating User Privacy in Bitcoin*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY: FC 2017 INTERNATIONAL WORKSHOPS 34 (Brenner et al. eds., 2013); *see also* Micha Ober, Stefan Katzenbeisser & Kay Hamacher, *Structure and Anonymity of the Bitcoin Transaction Graph*, 5 FUTURE INTERNET 237, 239–41 (2013) (stating that according to Bitcoin protocol, "the balance associated with an address cannot be divided into smaller amounts. Nevertheless it is possible to use the same input address again as output address; this way only a fraction of the balance can be transferred to another address, whereas the remainder of a balance can be transferred back to the originator. This has, of course, negative implications on privacy: it allows to link different transactions, as an attacker can more accurately estimate the number of active entities (if there was no linkability, the new transaction would look as if it originated from a new entity." The authors also mention that, in order to maximize both the anonymity set of Bitcoin and the unlinkability of transactions, "an entity that is observable by an adversary by inspecting the Bitcoin block chain should be as small as possible (best case: single address, increasing the anonymity set) and only active for a short time (best case: single transaction, limiting transaction linkability). There can be numerous reasons why this is not achievable in practice. First of all, addresses belonging to known public entities like mining pools are of course active for a very long time and it would not be of much use to obfuscate those addresses. On the other hand, a user mining on a pool with the same payout address all the time or some entity accepting donations on a single address will weaken the privacy of those entities. Even though the Satoshi Bitcoin client generates a new address for remaining change—which should strengthen privacy—as the user still receives funds on the old/original address, both addresses are likely to be used as inputs in some future transaction the user makes, which then

spreading data over multiple nodes may facilitate access to private data sets.[58] Distribution of private data over the ledger could violate data protection laws. Some jurisdictions have severe penalties for violations of data protection rules.[59] Entities using DLT must carefully and rigorously consider and address their data privacy obligations.

Another interference with privacy rights stems from the fact that data once stored on the ledger cannot be erased; this is DLT's immutability feature. This may have devastating consequences to an individual or entity. For instance, assume that inaccurate data on the credit worthiness of a person or illicit pictures of children and young adults are spread over the ledger. This is at odds with the "right to be forgotten" granted in some jurisdictions, so victims will turn to damages instead. More significantly, this is directly at odds with the requirements of law that in some circumstances transactions are void, and title must be rectified to reflect this, for instance, in the context of fraudulent transfers. Immutability and the requirements of law will clash.

b. Insider Trading and Market Abuse

If DLT is used to store sensitive, valuable information, it may facilitate a range of financial abuses, including insider trading, tipping, and market manipulation.[60] ESMA is concerned that the "shared and public features of DLT could facilitate market manipulation and other unfair practices. In the absence of proper safeguards, some could unduly exploit the information recorded in DLT, *e.g.*, recent trades or inventories levels of other participants, to front-run competitors or manipulate prices."[61] While civil and criminal penalties for insider trading and market abuse are severe,[62] responsible entities may also face

again allows a connection between the addresses to be made"); Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, *in* SECURITY AND PRIVACY IN SOCIAL NETWORKS 197, 221 (Yaniv Altshuler ed., 2013) (tracking the flow of Bitcoin transactions in a small part of a Bitcoin log); Matthew Elias, Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy 1 (Oct. 3, 2011) (unpublished manuscript) (available at https://ssrn.com/abstract=1937769) (stating that Bitcoin's system architecture is analogous to that of the internet so the level of anonymity is similar to that on the internet, but finding that "anonymity on the internet is a function of one's technical knowledge and ability, and of the amount of resources one is able to dedicate towards that end.").

58. Garry Gabison, *Policy Consideration for the Blockchain Technology Public and Private Applications*, 19 SMU SCI. & TECH. L. REV. 327, 330–35 (2016).

59. For instance, under the European Data Protection Regulation that has come into force in May 2017, regulators may impose penalties of up to 4% of a firm's turnover. *See* EUR. SEC. MKTS. AUTH., *supra* note 2, at 12, ¶ 42 ("ESMA realises that the use of DLT could in some cases raise privacy risks in relation to client data.").

60. *Cf.* Dorit Ron & Adi Shamir, *Quantitative Analysis of the Full Bitcoin Transaction Graph*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY: FC 2017 INTERNATIONAL WORKSHOPS 6 (Brenner et al. eds., 2013).

61. *See* EUR. SEC. MKTS. AUTH., *supra* note 2, at 11, ¶ 38.

62. *See* 15 U.S.C. § 78u–1 (2012) (providing civil penalties for insider trading and allowing the court to impose penalties three times the profit gained or loss avoided). Under European law, the penalties are even more severe, amounting to up to either 15% of the entity's turnover for insider dealing, unlawful disclosure, and market manipulation or €15 million, whatever is higher. *See* Market Abuse Regulation 596/2014, art. 30(2), 2014 O.J. (L 173) 1.

civil litigation in certain cases. Again, users of DLT will have to scrupulously guard against this abuse of the information on the system. This highlights another set of potential risks of the transparency characteristic of DLT.

c. Identity Theft

While transparency is beneficial to data integrity, it also facilitates access to assets through identity theft.[63] In particular, if only the private key is required to divert assets and no central ledger authority is able to block access upon notice of loss, the private key itself becomes the target of illicit activities.[64]

2. Cyber Risks

a. Tampering with Data Prior to Storage

Second, DLT does not solve the general issue of data processing: inaccurate data remain inaccurate however it is stored. For instance, if data from a financial transaction are stored on a distributed ledger, the data will often be generated by just two entities, buyer and seller. Attacking the (weak) input link rather than the distributed ledger itself will lead to inaccurate data being distributed. If a cyberattack focuses on the transacting parties rather than the storage device, *i.e.*, DLT, users relying on the ledger may not realize the inaccuracies and rely upon the data.[65] Permissionless distributed ledgers are particularly exposed due to nonexistent user/client enrollment/identity processes. With Bitcoin, the weakest link is the Bitcoin owner's wallet,[66] *i.e.*, the device in which the owner's value is booked and is exclusively held by the owner similar to a bearer instrument. For instance, in the Mt. Gox case, cyberattacks were directed toward the weak input link (*i.e.*, the exchange's "hot wallet," a set of data-holding keys for Bitcoin, which are used to handle day-to-day business)[67] rather than the ledger itself.

63. The technique is referred to as a Man-in-the-Middle Attack. Victoria Louise Lemieux, *Trusting Records: Is Blockchain Technology the Answer?*, 26 RECS. MGMT. J. 110, 128 (2016) ("Whenever one system passes information to another system, there exists a possibility for a Man-in-the-Middle Attack (MitMA). MitMA occurs when an attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other.").

64. Jennifer J. Xu, *Are Blockchains Immune to All Malicious Attacks?*, FIN. INNOVATION, Dec. 10, 2016, at 1, 6.

65. Again, this is likely to happen by virtue of a Man-in-the-Middle Attack. *See* Gabison, *supra* note 63, at 350.

66. *Cf.* Umeh, *supra* note 56, at 58; EUROPEAN BANKING AUTH., *EBA Warns Consumers on Virtual Currencies* (Dec. 12, 2013), https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies.

67. *Cf.* Christian Decker & Roger Wattenhofer, *Bitcoin Transaction Malleability and Mt. Gox*, *in* COMPUTER SECURITY—ESCORICS 2014: 19TH EUROPEAN SYMPOSIUM ON RESEARCH IN COMPUTER SECURITY 313, 318 (Miroslaw Kutylowski & Jaideep Vaidya eds., 2014).

b. Brute-Force Attack and Cheats

Even in what DLT is best at—safe storage—a distributed ledger has its limits. In particular, rules on how proof-of-work concepts determine consensus may reduce the reliability of the technology. For instance, in the blockchain that underlies Bitcoin, just five mining pools together process approximately 85% of all mathematical problems, *i.e.*, mining of coins.[68] The ledger is partly recentralized. If one attacks nodes that cover the required consensus level, then the chain could be compromised.[69] At the same time, in proof-of-stake systems, there is a central storage or processing device on which the stakes are calculated that could be targeted; thus, in a permissioned blockchain, a cyberattack could target the devices determining the governance of the blockchain, *i.e.*, the vote calculator, etc.[70] These are examples of a distributed ledger being broken by brute force, *i.e.*, by bundling computing power to attack multiple nodes simultaneously.[71] Since this requires an enormous amount of computing power—in theory, a Bitcoin attacker needs at least 51% *more* computing power than what the network already encompasses[72]—an attack may be more successful if it "convinces" the necessary number of nodes (or cheats those nodes) to adopt a different version of the ledger software through which the desired change is implemented.[73] In fact, if all attacked nodes are of the same level of security as a centralized ledger, a brute-force attack will require very significant effort

68. *BitCoin Mining Pools*, BITCOIN MINING, https://www.bitcoinmining.com/bitcoin-mining-pools (last visited May 16, 2018).

69. For instance, if a cyberattack targets the five most important nodes, it has a high probability of hitting the node solving the particular mathematical problem. Given that impact on consensus is based on data processing volume in the blockchain, it could influence the results, and as a result, would have the support from 85% of the distributed ledger.

70. *Cf.* Nicolas Houy, *It Will Cost You Nothing to "Kill" a Proof-of-Stake Crypto-Currency*, 34 ECON. BULL. 1038 (2014). On general governance issues, see David Yermack, *Corporate Governance and Blockchains*, 21 REV. FIN. 7, 10 (2017).

71. *See* Umeh, *supra* note 56, at 61 ("Although not totally impossible, such a hack is non-trivial, computationally prohibitive activity to execute over a large distributed peer network."). Umeh assumes the presence of private participants, while the reality may include state-coordinated groups of attackers with resources unlimited by economic constraints. *See* ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 213 (2014); Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 859–65 (2015).

72. *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN, https://bitcoin.org/bitcoin.pdf (last visited May 16, 2018) ("The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.").

73. For instance, modification of the Bitcoin blockchain requires a majority of nodes to consent to the change. The fact that ledger software is complex, and few node owners are computer literate, facilitates a cheat based on misinterpretation of the code. *See* Christopher, *supra* note 7, at 173–74; Walch, *supra* note 71, at 867–68; Yermack, *supra* note 70, at 10 ("Proposed changes to the Bitcoin blockchain code occur via a passive process of adoption or rejection by holders of more than 50% of the network's mining power, and in principle a change in the code can be initiated by anyone . . . this decentralization of authority over a blockchain might leave it vulnerable to sabotage. Rogue participants intent on crashing the network or diverting assets to themselves might propose software changes that appear benign and are widely adopted, or alternatively, might tempt others to adopt them using strategies based on the exploitation of collective action problems.").

from the attacker if all nodes are equally important and safe.[74] Yet both conditions are unlikely to be true.[75]

First, as was shown above, transaction logic will lead to concentration among the nodes, making some more important than others. For instance, in some virtual currency blockchains, nodes are compensated per transaction they complete, thus providing incentives to compete for transactions. Some of the most active nodes will process a high proportion of transactions, leading to a concentration of data generation on those nodes.[76] If consensus building is capacity oriented, as in some blockchains including Bitcoin, the attack must only result in control over more computing power than is retained by honest nodes,[77] an instance referred to as a "51% attack."[78] Thus, a cyberattack that focuses on the handful of nodes in which most transactions are concentrated is more likely to be successful.[79]

Second, some nodes will be safer than others because some owners will invest more in cybersecurity than others. It is safe to assume that the majority of nodes managed by nonprofessional institutions will be less secure than the cyber fortresses typical of important centralized ledgers. Rather than attacking all nodes in a distributed ledger where consensus is built, attacking the nodes with weaker security may be more productive with less effort than that required for a brute-force attack on all nodes simultaneously. These attacks promise better results when the attackers have access to any resource not available to oth-

74. Simon Barber, Xavier Boyen, Elaine Shi & Ersin Uzun, *Bitter to Better—How to Make Bitcoin a Better Currency*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY: 16TH INTERNATIONAL CONFERENCE 399, 399–414 (Angelos D. Keromytis ed., 2012).

75. *Cf.* Sindri Leó Árnason, Cryptocurrency and Bitcoin: A Possible Foundation of Future Currency Why It Has Value, What Is Its History and Its Future Outlook (June 2015) (unpublished B.Sc. essay, University of Iceland) (available at https://skemman.is/bitstream/1946/20840/1/BS%20Ritger%C3%B0%20-%20Cryptocurrency%20-%20Sindri%20Le%C3%B3%20%C3%81rnason%20Final.pdf).

76. Arthur Gervais et al., *Is Bitcoin a Decentralized Currency?*, IEEE SECURITY & PRIVACY, May–June 2014, at 54, 60 ("[While] [g]overnments and banks control almost every financial system; Bitcoin substitutes these powerful entities with other entities, such as IT developers and mining pool owners . . . . In this sense, Bitcoin now finds itself in unfamiliar territory: on one hand, the Bitcoin ecosystem is far from being decentralized; on the other, the system's increasing centralization doesn't abide by any transparent regulations or legislations."); Santiago Pontiroli, *Well, That Escalated Quickly: From Penny-Stealing Malware to Multi-Million-Dollar Heists, A Quick Overview of the Bitcoin Bonanza in the Digital Era*, VIRUS BULL. CONF., Sept. 2014, at 47; Joshua A. Kroll, Ian C. Davey & Edward W. Felten, The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries 11–13 (unpublished forum paper from the 12th Workshop on the Economics of Information Security, Georgetown University, June 23–24, 2013) (available at https://www.econinfosec.org/archive/weis 2013/papers/KrollDaveyFeltenWEIS2013.pdf); Kevin D. Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, BERKELEY TECH. L.J. (forthcoming 2018).

77. Nakamoto, *supra* note 72, at 1.

78. *See* Walch, *supra* note 71, at 861 (citing Bitcoin proponent ANTONOPOULOS, *supra* note 71, at 211–12).

79. ANTONOPOULOS, *supra* note 71, at 211–12; Safari Kasiyanto, *Security Issues of New Innovative Payments and Their Regulatory Challenges*, *in* BITCOIN AND MOBILE PAYMENTS: CONSTRUCTING A EUROPEAN UNION FRAMEWORK 145, 153–55 (Gabriella Gimigliano ed., 2016); Till Neudecker, Philipp Andelfinger & Hannes Hartenstein, *A Simulation Model for Analysis of Attacks on the Bitcoin Peer-to-Peer Network* 2015 IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT 1327, 1327 (Remi Badonnel et al. eds., 2015); Xu, *supra* note 64, at 5.

ers; one might think of advanced cryptoanalysis while the nodes' encryption has lower standards.[80]

c. Double Spending and Distributed Denial-of-Service Attacks

Further potential liability events have been discussed in the information technology literature. These include double spending attacks where the same currency unit is simultaneously assigned to two different users so that both are under the impression of having received, and are able to spend, the same coin at the same time.[81] One mechanism of self-defense foreseen by the Bitcoin core developers is that nefarious manipulation would lead to a general loss of trust that would result in Bitcoin's value plunging, thus presumably harming the attackers, who are presumably heavily invested in Bitcoin.[82] This disincentive is unlikely to stop attackers seeking to destroy the Bitcoin system "as a form of terrorism,"[83] or merely to harm its users.[84]

Another potential threat stems from distributed denial-of-service attacks ("DDOS"). Again, DDOS is more dangerous the more concentrated the ledger. For instance, in the Bitcoin ledger where a handful of mining pools control by far the most computing power, DDOS attacks could bring, and have frequently brought,[85] mining to a halt, interfering not only with the core system of predictable new Bitcoin creation, but also holding up transfers users were planning to conduct during this period. The more widely spread DLT is in the business sector, the more likely it is that some rogue or terrorist may turn to DDOS. Even if immediately detected due to intense monitoring, the effects are potentially severe. For instance, in the case of Bitcoin, the BTC exchanges closely monitor every move of every BTC made. In the case of detection, exchanges tend to cease operations (in order to protect themselves), and the value of BTC is likely

80. Crosby et al., *supra* note 22, at 12–13; Walch, *supra* note 71, at 864; Danny Yuxing Huang et al., Botcoin: Monetizing Stolen Cycles 1 (2014) (unpublished manuscript) (available at https://www.cs.princeton.edu/~yuxingh/static/ndss14-cr.pdf); James Wyke, *The ZeroAccess Botnet—Mining and Fraud for Massive Financial Gain* 9 (Sept. 2012) (unpublished technical paper, SophosLabs) (available at https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/Sophos_ZeroAccess_Botnet.pdf).

81. *Cf.* ANTONOPOULOS, *supra* note 71, at 211–12; Nakamoto, *supra* note 72, at 7; Ghassan O. Karame, Elli Androulaki & Srdjan Capkun, Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin 1 (2012) (unpublished manuscript) (available at http://eprint.iacr.org/2012/248.pdf) (demonstrating that double-spending attacks on fast payments can be mounted at low cost on the then-deployed versions of Bitcoin and that "the measures recommended by Bitcoin developers for the use of Bitcoin in fast transactions are not always effective in resisting double-spending," and proposing countermeasures that enable the detection of double-spending attacks in fast transactions).

82. Nakamoto, *supra* note 72, at 4.

83. ANTONOPOULOS, *supra* note 71, at 211–12; Christopher, *supra* note 7, at 176 (citing Jörg Becker et al., *Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency*, *in* THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY 135, 150 (R. Böhme ed., 2013)).

84. *Cf.* Walch, *supra* note 71, at 862 (citing ANTONOPOULOS, *supra* note 71, at 212–13).

85. For instance, in the week of March 7, 2015, five Bitcoin mining pools were subject to a DDOS attack that prevented miners from mining for six hours. The attacker demanded five to ten bitcoins to end the attack. *See* Julia McGovern, *Official Statement on the Last Week's DDoS-Attack Against GHash.IO Mining Pool*, CEX.IO BLOG (Mar. 16, 2015), https://blog.cex.io/news/official-statement-on-the-last-weeks-ddos-attack-against-ghash-io-mining-pool-14156.

to drop.[86] As long as the operational deficiency prevails, it would be extremely difficult to move the BTC from virtual currency to fiat currency. Clients whose assets were frozen will ask for reimbursement of their costs.

3. Operational Risks

a. Insufficient Coding

While the standardization and automatization that form part of DLT mitigate—in principle—operational risk, an error implemented in the code may easily spread over the whole system, affecting a greater number of nodes and individuals than a concentrated ledger.[87] This creates serious problems in light of the fact that "there is no such thing as flawless software; there are always errors or 'bugs' that negatively affect the performance of the software or make it vulnerable to attack by hackers."[88]

In particular, poorly maintained, outdated, or deficient code could open the door for system hacks, such as those that occurred in the Mt. Gox and DAO cases.[89] Further, the governance deficiencies of permissionless ledgers may turn into real-world issues in the context of insufficient coding. For instance, the hard fork that occurred in the Bitcoin system on August 1, 2017 was due to a lack in consensus as to whether a specific update improved the system or led to unqualified benefits of some users.[90]

b. Key Person Risk

Distributed ledgers rely on sophisticated software codes that are permanently rewritten in an effort to improve performance and security.[91] As with all software, few experts understand the structure, and even fewer are able to adapt it if weaknesses of the code become known. This is particularly true in the case of permissionless ledgers, such as Bitcoin, where

> [a] small group of core developers [have] password access to the code. They review and evaluate the suggestions made by other programmers, incorporate what they consider to be the good suggestions, and promulgate revised versions of the code for network adoption. They approve small changes by fiat, but for larger ones they moderate a public debate about the utility of the change. This bottleneck of human oversight does

86. Amir Feder, Neil Gandal, JT Hamrick & Tyler Moore, *The Impact of DDoS and Other Security Shocks on Bitcoin Currency Exchanges: Evidence from Mt. Gox*, 3 J. CYBERSECURITY 137, 138 (2017).

87. *See* EUR. SEC. MKTS. AUTH., *supra* note 2, at 11, ¶ 38.

88. *See* Walch, *supra* note 71, at 856. This is particularly true for the software underlying the Bitcoin system. *See id.* at 858 & n.99–102 (detailing a list of bugs and identified fixes). The statement counters the open source mantra according to which "the more eyes look at the code the more can fix and react."

89. *See* Xu, *supra* note 64, at 6.

90. *See* Tom Simonite, *Bitcoin is Spliting in Two. Now What?*, WIRED (Aug. 1, 2017), https://www.wired.com/story/bitcoin-is-splitting-in-two-now-what.

91. *See* Walch, *supra* note 71, at 865–67.

> not fit the narrative of central-bank-less currency, which may be why many advocates avoid discussing it.[92]

Even if the risk is mitigated in the Bitcoin ledger because all of the code is being made public,[93] the core concern holds true: in all business organizations, key people pose a risk to the organization—they could become sick, tired, mentally unwell, or subject to extortion or corruption.[94] Regardless of the reason, if the trust put in key people is ill-placed, the ledger's security and reliability are at risk. This general risk may be increased in some distributed ledgers (such as Bitcoin) if the key people in charge fail to convince a sufficient number of users to update their version of the code, resulting *de facto* in a loss of key person capacity and an uncertain future of the ledger.[95] If this happens, questions will be asked as to who is accountable for the key person's underperformance or misconduct.

c. Negligent Performance

For large-scale financial services data, security and processing speed are of the essence. Assuming that a distributed ledger ensures certain security and processing standards to market participants in an effort to enhance market share, the question of who is responsible will be asked if the ledger fails to meet these standards. Another example of negligent performance (in this case, on the user's side[96]) is the user sending virtual currency to the wrong address; is there anyone to whom the user can turn for redress?[97]

B. Legal Consequences

Even in light of its limits, DLT is likely the safest way to ensure that data are not modified. At the same time, DLT's limits lead to legal questions. In particular, if a system is broken or inaccurate, or if private data are stored via a distributed ledger, the legal question of who will be liable for losses will arise.

This question is not easy to answer given that DLT is a technological, not a legal, concept. Operating a blockchain tells us, in the first instance, nothing about the legal scheme underpinning the blockchain. This has several implications.

92. *See* Christopher, *supra* note 7, at 150; *see also* Grinberg, *supra* note 7, at 175–76.

93. *Cf.* ANDREW O'HAGAN, THE SECRET LIFE: THREE TRUE STORIES OF THE DIGITAL AGE 113–218 (2017) (arguing that key people risk is mitigated in the Bitcoin ledger due to the fact that developer Gavin Andresen made the code public in 2011).

94. *See* Walch, *supra* note 71, at 860–61 (citing Bitcoin proponent ANTONOPOULOS, *supra* note 71, at 157, 211).

95. *See* Lulu Yilun Chen & Yuji Nakamura, *Bitcoin Is Having a Civil War Right as It Enters a Critical Month*, BLOOMBERG (July 11, 2017, 6:53 AM), https://www.bloomberg.com/news/articles/2017-07-10/bitcoin-risks-splintering-as-civil-war-enters-critical-month ("After two years of largely behind-the-scenes bickering, rival factions of computer whizzes who play key roles in bitcoin's upkeep are poised to adopt two competing software updates at the end of the month. That has raised the possibility that bitcoin will split in two, an unprecedented event that would send shockwaves through the $41 billion market.").

96. JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 10 (2016).

97. Example taken from Christopher, *supra* note 7, at 176.

1. Applicable Law

First, very few governments have as yet adopted a *Blockchain law*.[98] That does not mean, however, that no law applies or, as has been stated, that the law's focus needs to shift from individuals to (web) communities[99]—we pesky lawyers cannot be so easily sidelined. Rather, lawyers facing innovation look at the legal system as a whole and apply the system's foundational principles.[100] And the law will provide an abundance of generally applicable principles, including the law of contracts, torts, property, and partnerships and companies, some of which are enshrined in legislation while others (particularly in common law countries) are in case law which applies in the absence of specific legislation. Applying law to DLT will not be about "uncovering a functional equivalent—another [legal] institution that, although different in structure, serves the same purpose . . . ,"[101] but will entail applying general principles in the absence of specific legislation.[102]

2. Ledger Hierarchy

Second, DLT tells us nothing about the *entities involved* or their *governance roles*. For instance, multiple servers functioning as nodes can belong to one legal entity (firm or person) or financial group, or they can belong to multiple unrelated owners. With regard to governance, in the case of permissionless blockchains, node owners typically will not even know who else is part of the blockchain, and a more-or-less "benevolent dictator"[103] will make the deci-

98. Arizona has adopted a blockchain law. ARIZ. REV. STAT. ANN. § 44-7061 (2018). Others are considering.

99. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999) (arguing in favor of adaptation of the law to cyberspace); Dulong de Rosnay, *Peer-to-Peer*, *supra* note 24 (positing that "distribution of actors and actions requires a rethinking of legal categories, since the notions of the author of an action, action and content or object are no longer tangible units, but aggregated, open-ended and evolving fragments."). The author, however, confuses law with its enforcement. The facts mentioned may render enforcement difficult, but do not change the fact that the law assigns rights and liabilities even in a distributed system. For enforcement difficulties due to irreversibility of the blockchain, see Paech, *supra* note 17, at 1109.

100. RICHARD A. EPSTEIN, SIMPLE RULES FOR A COMPLEX WORLD 21–22 (2009) (stating that principles are well equipped to govern complex technical concepts); Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 213 (1996) (demonstrating the importance of principles); Raskin, *supra* note 19, at 972 ("[N]ovel problems do not require novel solutions."). *But see* Paech, *supra* note 17, at 1094–95, 1100 (stating that system issues render enforcement difficult, implying that legal claims are granted by the law, and demanding that de facto acquisition on the basis of the operation of software needs to be recognized by private law itself—without further details).

101. Reyes, *supra* note 1, at 222–27 (summarizing comparative law methodology and suggesting an endogenous, functional approach).

102. For instance, U.S. courts and criminal enforcement agencies rigorously enforced criminal laws against Silk Road's mastermind Ross William Ulbricht, fitting Bitcoin into existing jurisprudence. *See* references cited *supra* note 19.

103. David S. Evans, *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms*, 15–16 (Coase-Sandor Inst. for Law & Econ., Working Paper No. 685, 2014), http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2349&context=law_and_economics (referring to the general structure underlying open source technology).

sions (or more precisely, "dictators," since a group of core developers will tend to call the shots). A permissioned blockchain, on the other hand, may have highly developed and legally sophisticated governance structures.

For the purpose of generalization, we rely on a DLT hierarchy involving five groups:

1. the "core group" that sets up the code design and (*de facto*) governs the distributed ledger (for instance, by having the technical ability and opinion leadership to prompt a "hard fork" of the system (under certain conditions));[104]
2. the owners of additional servers running the distributed ledger code for *validation purposes* (such as Bitcoin node owners, Ripple validation nodes, etc.),
3. "qualified users" of the distributed ledger (such as exchanges, lending institutions, miners, etc.);[105]
4. "simple users" of the system (such as owners of Bitcoin,[106] Ether, or investors in the DAO); and
5. third parties affected by the system without directly relying on the technology (for instance, counterparties of, and banks lending to, "simple users," clients of intermediaries that clear their financial assets via DLT, clients of brokers that hold virtual currency on behalf of clients, etc.)

FIGURE 2: LEDGER HIERARCHY

104. As an example, see Antonio Madeira, *The DAO, the Hack, the Soft Fork and the Hard Fork*, CRYPTOCOMPARE (Jan. 12, 2018), https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork. For further examples, see Christopher, *supra* note 7, at 150; Grinberg, *supra* note 7, at 175–76. The U.S. Financial Crime Enforcement Network applies its AML rules to "administrators and exchangers" of "convertible virtual currencies." *See* Comizio, *supra* note 6, at 141. Although FinCEN does not mention the core developers, we deem "administrators" to include core developers.

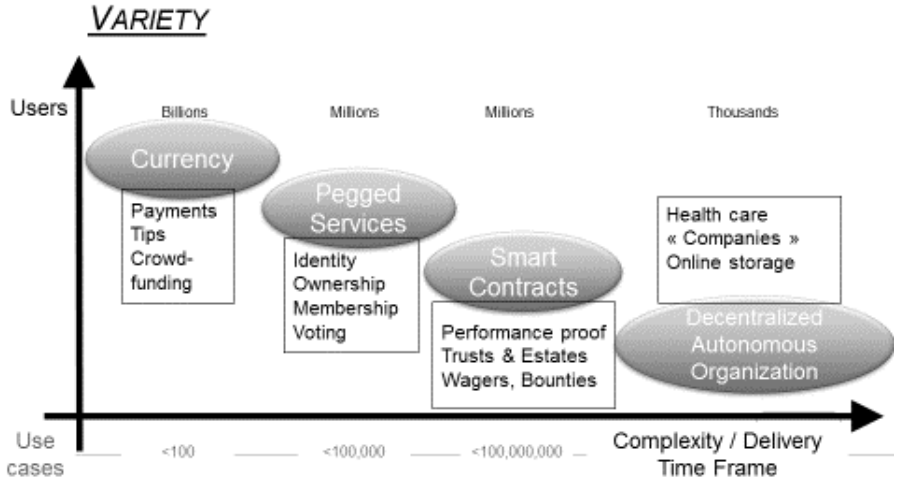
105. The U.S. Financial Crime Enforcement Network applies its AML rules to "administrators and exchangers" of "convertible virtual currencies." *See* Comizio, *supra* note 6, at 141. "Exchangers" include all qualified users in this sense. On the role of intermediaries in the Bitcoin blockchain, see Christopher, *supra* note 7, at 151, 174.

106. In the Bitcoin ledger, validation nodes (element 2) and owners (element 3) are identical.

3. Variety

Third, DLT is a concept with *multiple variations*. From a distance, Bitcoin, Ethereum, R3, and Ripple are all built on DLT, so one is tempted to generalize. But up close, they are very different animals. Generalizations are not warranted. Each DLT serves a certain use case, which ranges from currency, pegged services, and automatic execution of functions to permanent organizations.

FIGURE 3: BLOCKCHAIN APPLICATIONS: END-USER VIEW[107]



Depending on the DLT's design and use case, the number of users, the technical complexity, and the delivery timeframe will vary—and so will the legal questions. As a result, when considering DLT from the accountability perspective, it is crucial to:

1. determine the governance structure and entities involved;
2. clarify which legal standards apply to which DLT processes and services;
3. ensure the robustness of the IT processes given their great importance for the existence of the firm (from "important" to "indispensable"), leading to enhanced regulatory attention regarding server infrastructure, redundancy, access rights, server location, etc.;
4. ensure that the algorithms achieve "correct" results, requiring regulators to define which documentation (or data interfaces) need to be pro-

107. Taken from William Mougayar, *Understanding the Blockchain*, O'REILLY (Jan. 16, 2016), https://www.oreilly.com/ideas/understanding-the-blockchain.

vided by intermediaries, which test routines must be embedded in the algorithms, and who has access to the source code and data bases used; and

5. clarify liability and responsibility for failure of the IT systems and algorithms.

The remainder of this section focuses on the fifth question.

C. Joint Control as Legal Qualification of a Blockchain

If we factor in liability, embedding DLT in financial transactions may produce results that many will find surprising. A DLT entity (whether operator or participant) may need regulatory capital, counterparty risk controls, and other measures similar to other forms of financial infrastructure (such as central counterparties). In turn, the legal design of the DLT may look different from the technological design—for instance, ownership may be distributed, concentrated, or centralized.

1. Code as Law?—The Debate

There is a lively debate as to whether "software code is law."[108] Three perspectives are relevant here.

First, Lawrence Lessig originally meant "code is law" as a metaphor "in that the code controls behavior as law might control behavior."[109] Code design and structure will define the freedom of users: the code will determine what users can and cannot do, and what they must and must not do when using the system. This will be particularly so in the machine-based interactions often referred to as smart contracts.[110] Furthermore, some legislatures, such as that of

108. To our knowledge, the discussion dates back to Lawrence Lessig's seminal book CODE AND OTHER LAWS OF CYBERSPACE 3–8 (1999). Lawrence Lessig, *Foreword,* 52 STAN. L. REV. 987, 989–90 (2000) [hereinafter Lessig, *Forword*]; Lawrence Lessig, *Open Code and Open Societies: Values of Internet Governance*, 74 CHI.-KENT. L. REV. 1405, 1408 (1999) [hereinafter Lessig, *Open Code and Open Societies*]. From a legal perspective, the statement is ill-received. Statutes and cases comprise law; code can only be the subject of law. Legal authors tend to use the variant "code-as-law." *See* Reyes, *supra* note 1, at 196.

109. Lessig, *Foreword*, *supra* note 108, at 990; Lessig, *Open Code and Open Societies*, *supra* note 108, at 1408 ("The code of cyberspace—whether the Internet, or a net within the Internet— defines that space. It constitutes that space. And as with any constitution, it builds within itself a set of values and possibilities that governs life there. . . . And the design of code is something that people are doing. Engineers make the choices about how the world will be. Engineers in this sense are governors.").

110. On smart contracts, see the pioneering work by Nick Szabo, *A Formal Language for Analyzing Contracts*, U. AMSTERDAM (2002), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/contractlanguage.html (last visited may 16, 2018); Nick Szabo, *The Idea of Smart Contracts*, U. AMSTERDAM (1997), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (last visited May 16, 2018). *See also* Merit Kõlvart, Margus Poola & Addi Rull, *Smart Contracts*, *in* THE FUTURE OF LAW AND ETECHNOLOGIES 133, 133 (Tanel Kerikmäe & Addi Rull eds., 2016); Baker, *supra* note 6, at 360–63; Anthony J. Casey & Anthony Niblett, *Self-Driving Contracts*, 43 J. CORP. L. 1, 2 (2017); Joshua Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35, 38 (2014); Riikka Koulu, *Blockchains and Online Dispute Resolutions: Smart Contracts as an Alternative to Enforcement*, 13 SCRIPTED 40, 41 (2016); Karen E. C. Levy, *Book-Smart, Not Street-Smart: Block-*

Arizona, have clarified that smart contracts are as legally effective as other contracts by enacting legislation giving legal status to smart contracts and blockchain-based signatures, treating them as any ordinary contract or signature.[111] In turn, contract law applies to blockchain-based contracts, removing any uncertainty and making it clear that any blockchain-based agreement is fully enforceable in court.

The second dimension includes the question of who owns the distributed ledger software code; this is a question of property or copyright law and the legal protection of designs. The answer may have repercussions, however, as to the question of who is responsible for the code from a tort law perspective, addressed in Subsection III.D.2 below.

The third perspective relates to the question of the legal treatment of the cooperation underlying a distributed ledger. This analysis questions whether those cooperating in a system are liable for failures and who among all the various nodes bears the legal responsibility for system hacks. These questions are of particular importance regarding the legal design of a distrusted ledger system; the remainder of this section addresses these questions.

We will focus on the third issue of whether there are legal grounds for liability before arguing against the "code-is-law" argument as a defense against the liability claim (if any), which is considered in more depth in Subsection III.D.5.

2. Application of Law to the Distributed Ledger

Regarding the question of the legal treatment of the cooperation underlying a distributed ledger, the type of cooperation created by code is of legal relevance:[112]

First, in general, law covers all relations among people and items owned and controlled by them. There is no carve-out for cooperation in a distributed ledger.

Second, no legislature is likely to enact an exception to this catch-all characteristic of law as it would promote irresponsible behavior by those con-

chain-Based Smart Contracts and the Social Workings of Law, 3 ENGAGING SCI., TECH. & SOC'Y 1, 1 (2017); Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 313 (2017); Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia 10–12 (March 12, 2015) (unpublished manuscript) (available at https://ssrn.com/abstract=2580664); Cheng Lim et al., *Smart Contracts: Bridging the Gap Between Expectation and Reality*, OXFORD BUS. L. BLOG (July 11, 2016), https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality.

111. *See Arizona Gives Legal Status to Blockchain Based Smart Contracts*, TRUSTNODES (Apr. 3, 2017, 4:32 PM), http://www.trustnodes.com/2017/04/03/arizona-gives-legal-status-blockchain-based-smart-contracts ("A signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature. A record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record. Smart contracts may exist in commerce. A contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term.").

112. *See* Koulu, *supra* note 110, at 54.

trolling the distributed ledger. No legal system could afford a carve-out for DLT interactions given the loopholes it would create.

Third, the discussion as to whether human beings are responsible for machines is of long-standing importance, at least since the industrial revolution. In all jurisdictions of which we are aware, the answer to this question has been the same: the law will cover, and be applied to, new situations and inventions appropriately modified to the new circumstances.

Further, individual transactions executed via a distributed ledger are likely to be contracts—with all related consequences—whether recorded only in code or in words. Each transaction is likely to give rise to liability in the event of failure; which will sound in real-world obligations and potentially in bankruptcy.

The fact that law will apply is to be distinguished from the question of *which* law will apply. This will be determined by the application of the conflicts of law rules of the courts with potential jurisdiction over the matter, including their treatment of any choice of law provision in any agreement establishing the DLT.[113]

3. Distributed Ledgers vs. Business Networks

From the outset, one is inclined to liken distributed ledgers to traditional "business networks" (such as franchise systems, credit card networks, and supply chains involving multiple parties). Distributed ledgers, however, differ from such traditional hybrid organizations[114] in one important respect: while all members of the network (*e.g.*, franchisor and franchisees) are linked together by the common business interest (for instance, in the brand appeal), from a legal perspective, traditional business networks follow the hub-and-spokes model, where the spokes (*e.g.*, the franchisees) are only connected to the other spokes indirectly through a contractual relationship to the "hub" (for instance, the franchisor). The fact that the legal connection is indirect merely functions as a legal barrier: rather than treating the whole operation as one multilateral contract or business organization due to their economic connection,[115] all contracts between the hub and the spokes have only bilateral effect. This prompts

113. ADRIAN BRIGGS, PRIVATE INTERNATIONAL LAW IN ENGLISH COURTS 537–46 (2014). *See generally* DICEY ET. AL., DICEY, MORRIS & COLLINS ON THE CONFLICT OF LAWS (2016). On choice of law in the blockchain context, see LAW SOC'Y OF H.K., *supra* note 1, at 10–13.

114. Hugh Collins, *Introduction* to GUNTHER TEUBNER, NETWORKS AS CONNECTED CONTRACTS 1, 11 (Hugh Collins ed., Michelle Everson trans., 2011).

115. This was suggested by Teubner. GUNTHER TEUBNER, NETWORKS AS CONNECTED CONTRACTS 145 (Hugh Collins ed., Michelle Everson trans., 2011). His position finds support in scholarship. *See, e.g.*, THE ORGANIZATIONAL CONTRACT: FROM EXCHANGE TO LONG-TERM NETWORK COOPERATION IN EUROPEAN CONTRACT LAW 12–13 (Stefan Grundmann, Fabrizio Calaggi & Giuseppe Vettori eds., 2013); Roger Brownsword, *Network Contracts Revisited*, *in* NETWORKS: LEGAL ISSUES OF MULTILATERAL CO-OPERATION 31, 31 (Marc Amstutz & Gunther Teubner eds., 2009); Gillian K. Hadfield, *Problematic Relations: Franchising and the Law of Incomplete Contracts*, 42 STAN. L. REV. 927, 976 (1990). To our knowledge, however, this approach has not received general support by the courts. For an analysis of the English courts' case law, see Collins, *supra* note 114, at 35.

three consequences. First, one spoke has no legal standing to sue another spoke for unfaithful conduct regarding the common objective. In a hub-and-spoke network, in the absence of contracts with explicit third-party benefits defined, there is no loyalty owed to the network, and in principle, courts are reluctant to find implied terms based on loyalty to the overall organization, fair dealing, "business necessity," and standard business practice.[116] Second, legal action must follow the path predefined by contractual relationships. In the absence of explicit bilateral contracts, parties to a network cannot bring economic claims against each other. In particular, one spoke cannot recover pure economic loss "horizontally" (*i.e.*, from the other spoke rather than the hub). The spoke sued will invoke the doctrine of privity of contract and challenge in tort law the standing of the claimant.[117] Third, there is no external liability of "the network" *vis-à-vis* third parties; rather, each spoke and the hub will be treated separately, and liability must be established against them individually.[118]

By contrast, rather than indirectly through a hub, in a distributed ledger all nodes (group two of our hierarchy) are linked together, meaning they communicate together in the consensus process and thereby determine which data stored via the "the common ledger" are right and wrong.[119] This connection removes the hierarchical relation derived from the hub-to-spoke characteristic for business networks and justifies the term "peer-to-peer networks."[120] In turn, we find no difference between horizontal and vertical anymore—all links to other nodes are by definition "on the same level," pursuing a common objective. From a legal perspective, the connection provides the link (or in business networks, "missing link") between the network partners. Where traditional business networks are mere virtual networks, distributed ledgers are "real" networks—with a real physical (tech) link. While distributed ledgers vary in terms of software processes, and thus their legal qualification is likely to vary, we posit that legal consequences follow from this direct link among the nodes:

116. For examples of franchise systems, see *Taylor Equip., Inc. v. John Deere Co.*, 98 F.3d 1028, 1029 (8th Cir. 1996) (finding that the implied duties of good faith and fair dealing do not override express terms); Burger King Corp. v. Family Dining, Inc., 426 F. Supp. 485, 492 (E.D. Pa. 1977), *aff'd*, 556 F.2d 1168 (3d Cir. 1977) (arguing in favor of a strict interpretation in a case where the franchisee had, with significant investment, opened nine franchise stores where his contractual obligations amounted to opening ten stores); Bak-A-Lum Corp. of Am. v. Alcoa Bldg. Prods., Inc., 351 A.2d 349, 352 (N.J. 1976) (stating that implied duties override express provisions in cases of extreme dishonesty and unfairness and extreme losses on the side of the franchisee); *Seven Eleven Corp. of S. Afr. (Pty) Ltd. v. Cancun Trading No. 150 CC* 2005 (2) All SA 256 (SCA) at 33–34 (S. Afr.) (limiting the rebates to be distributed under a rebate sharing agreement with franchisees to rebates granted for bulk purchases, assigning other rebates and soft commission to the franchisor); *Dymocks Franchise Sys. (NSW) Pty. Ltd. v. Todd* [2002] UKPC 50 (N.Z.) (finding an implied term of good faith that prevents the franchisee to call other franchisees for a strike). The courts' reluctance regarding implied obligations has prompted criticism, for instance, in Hadfield, *supra* note 115, at 970.

117. Collins, *supra* note 114, at 14–15, 51–63 (citing English and German case law).

118. *Id.* at 64–71.

119. Note that while depending on the server protocol and storage algorithm, there may be difficulties to prove that any node *X* was *directly* in contact with any node *Y*, any node *X* runs code with which node *Y* was, or necessarily comes, in contact.

120. *See* DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS MONEY, BUSINESS, AND THE WORLD 6 (2016).

it is the tipping point at which a loose assembly of self-interested entities turns into a group of entities legally tied together.

4. "Shared Control" as a Common Feature of Distributed Ledgers

The very fact of distribution among many ledgers that together perform a commercially relevant function renders legal consequences likely. At the same time, the joint performance assigns to all nodes together significant influence over all users' positions in that they can together exclude any single user from participation. For instance, if all but one user uploads a new software version incompatible with the old one, the value of the remaining user's position in the ledger suffers.[121] In most systems, agreement among a 51% majority of nodes or computing power is determinative. The operations of the information technologies interacting in a distributed ledger could be treated like those of the human beings controlling the servers and computers on which the software runs, or they could be treated like items a person is responsible for, similar to an animal or a car. In this case, the law would ask whether the person engaged in negligent conduct (*i.e.*, violated a standard of care when the item inflicted harm on someone).

We infer from such quasi-organizational characteristics of the distributed ledger, which go beyond mere economic interest, that the whole ledger has a purpose or aim—the joint performance of the ledger service—from which obligations to cooperate and of loyalty, as well as internal and external liability, could follow.

For instance, the distributed ledger could be deemed a *joint venture*. The core group that sets up the system is a clear potential example, but this could extend further; for instance, if nodes contribute and benefit to the same extent as the core group, even "simple users" could be deemed joint venturers by third parties that rely on their service. One could also understand the joint performance to constitute a *multi-party contract*, with the core group and all nodes functioning as contractors that commit to adhere to the processing rules and maintain a certain level of security. If the core group fails to deliver, or one or more of the nodes does not perform the necessary processes or does not maintain the minimum data security level, the fellow contractors could rely on contractual liability. In some jurisdictions, we may also find sufficient ground to argue that the distributed ledger is an *incorporated business organization* or *partnership*.

Once it is established that distributed ledgers have a sufficiently close organizational relation (regardless of how this is legally interpreted in any given

121. On March 11, 2013, an inadvertently created hard fork due to incompatibility of Bitcoin 0.7 with Bitcoin 0.8 almost destroyed value stored in the Bitcoin blockchain. The core developer convinced one significant exchange to reinstall the old version. The exchange controlled sufficient computing power within the Bitcoin's system to shift the majority consensus back to version 0.7. *See* NATHANIEL POPPER, DIGITAL GOLD: BITCOIN AND THE INSIDE STORY OF THE MISFITS AND MILLIONAIRES TRYING TO REINVENT MONEY 194–95 (2015); Gruber, *supra* note 20, at 164; Walch, *supra* note 71, at 865–67. This example is evidence of both the importance of core developers and the concentration of computing power in the Bitcoin blockchain.

jurisdiction), duties based on good faith as determined by the common good, liability among the ledgers (*i.e.*, internal network liability), and liability to third parties (*i.e.*, external network liability) could be presumed to arise. In turn, one node owes to the other nodes a duty of loyalty (for instance, not to turn off the computer in order to maintain the network's processing efficiency or regular software and hardware updates to maintain the ledger's performance) and is directly liable for economic loss in case of its breach. Further, if a third party is damaged by inaccurate or insecure data storage, which, as was shown,[122] is possible, the third party could direct its claim based on *tort law* or *special liability statutes*[123] to all nodes together.

This preliminary result arises in light of the six features of distributed ledgers,[124] including:

1. joint access to data ("distributed");
2. joint information about the process ("publicity" / "transparency");
3. joint administration (in that no single ledger alone can determine the outcome) ("decentralized");
4. joint development (*i.e.*, to change the underlying code, some consensus mechanism is necessary, and no single node alone can determine the outcome);
5. permanence—data cannot be erased, and a permanent log is maintained in which all transactions may be tracked by order of processing; and
6. verifiability—the above features combine to mean data cannot be amended while stored except through a major, trackable process ("immutability").

From a legal perspective, some type of liability—joint, several, or proportionate—could arise from this joint control toward third parties and among the nodes themselves. Which type of liability will arise will depend on the details of the DLT system, in particular, the consensus mechanism and the rules of the specific applicable legal system or systems. Our baseline position, however, is that there are significant potential liability risks for entities involved in a distributed ledger, particularly those with design, control, or maintenance roles.

D. Liability Risks in Major Legal Systems

Given that private law differs from country to country, we will address the three main legal families in the world, including French civil law based on the Code Civil (which extends to many Western European, African, and South

122. Walch, *supra* note 71, at 853.

123. In some common law countries, special liability statutes were implemented to provide a greater degree of certainty in the field of tort law. *See infra* Subsection II.D.2.

124. *See* DuPont & Maurer, *supra* note 5 (arguing that key characteristics of a blockchain include that the ledger is "distributed, decentralized, public or transparent, time-stamped, persistent, and verifiable").

American countries), common law (as examples we address the United States, the United Kingdom, and Australia), and Germanic civil law (which, besides Germany, is influential in Austria, the Netherlands, Switzerland, China, Japan, and Turkey).

We consider liability that may arise in one of four ways: (1) contract, (2) tort, (3) partnership or joint liability, and (4) specific legislation. Of course, the specifics of each head of liability will be entirely jurisdiction-specific, so our analysis is general and intended to do no more than make the point that participants in a distributed ledger are highly likely to be potentially subject to liability, one way or another, for their conduct. Proponents of DLT often like to pretend that the technology is somehow beyond the law, or at least the law's reach. But courts will never allow such a restriction in their jurisdiction. The courts of sophisticated legal systems are jealous of the extent of their jurisdictions for the very good reason that citizens should not be without redress in their nation's courts.[125] The result is that rather than not being subject to the law anywhere, DLT may instead be subject to the law everywhere.

1. Contract

In contract law, each party is liable under the terms of the contract, *i.e.*, for that which the contract says they are liable. The parties to the contract are not the computers as non-human electronic agents, but the people who exercise control (by virtue of ownership, management rights, or otherwise) of the non-human agent. The contractual acts—meeting of minds, breach of contract, performance—are attributed to this socio-technical ensemble.[126] To establish liability, a contract and a breach of the contract are required.

Without doubt, both contract and breach may be established (and have been established[127]) in the relationship between groups two through four of our distributed ledger hierarchy on the one side, and group five—the third parties—on the other. For instance, if the Bitcoin broker breaches its promise to hold a certain amount of virtual currency on behalf of its client, the broker will be subject to a contractual claim by its client.[128]

125. IRB-Brasil Resseguros, S.A. v. Inepar Invs., 982 N.E.2d 609, 610 (N.Y. 2012). *See generally* Owners of Cargo Lately Laden on Board Ship or Vessel Eleftheria v. The Eleftheria (Owners), The Eleftheria [1969] All ER 641 (Eng.).

126. Gunther Teubner, *Rights of Non-Humans? Electronic Agents and Animals as New Actors in Politics and Law*, 33 J. L. & SOC'Y 497 (2006).

127. The Bitcoin-denominated Ponzi scheme run by Trendon Shavers, who defrauded investors out of more than 700,000 Bitcoins, and the respective SEC enforcement action resulted in an order to disgorge investments amounting to more than US$40 million and a civil penalty of US$150,000 to be paid by both Shavers and the investment vehicle set up by him. *See* SEC v. Shavers, No. 4:13-CV-416, 2014 WL 4652121, at *13 (E.D. Tex. Sept. 18, 2014). Shavers, Securities Exchange Act Litigation Release No. 23090, 109 SEC Docket 17 (Sept. 22, 2014).

128. LAW SOC'Y OF H.K., *supra* note 1, at 85–87 (discussing liability of token issuers and redemption requirements); Bayern, *supra* note 21, at 25–29.

Beyond this obvious case, contractual relations extend further into the direct relationships among groups one to four of our DLT hierarchy, given that both contract and breach can be established.

A *contractual agreement* requires an offer and acceptance (to establish mutual assent), consideration (anything of value exchanged), and an intention to create legal relations.[129] As to offer, acceptance, and mutual assent, in our DLT hierarchy, we suggest that hierarchy groups one and two—the core group and validation nodes—are parties to the "distributed ledger contract" given that the system would not work without them.[130] Even if some members of DLT hierarchy groups one and two do not wish to enter into legally binding relations, the fact they participate in the system knowing that third parties will rely upon it may turn their participation in the distributed ledger into legally consequential conduct.[131] In particular, in the Bitcoin blockchain, individuals who wish to participate in the ledger join the network—and declare their consent to the disclosed *modus operandi*—by downloading the freely available Bitcoin software and thus volunteering their computer to run the Bitcoin ledger software.

Contract consideration matters in most common law systems. While consideration may be less readily identifiable given the uncertain flows of assets in open-source and permissionless systems, any type of consideration will suffice. Consideration can take many forms, including additional virtual assets (as in the case of Bitcoin miners), traffic on a website (for advertisement purposes), or fee payments. The fact participants willingly enter into a distributed ledger suggests that they perceive value from doing so. And, of course, in civilian legal systems, consideration is not usually a precondition for the existence of a contract.[132]

Second, whether there is a breach of contract depends on conduct in the context of the contract's terms. General principles of contract law apply: whether a term is a condition or a warranty depends on the intentions of the party, discerned from the contract in light of context. The more important such features are for one party, and the more clearly they are expressed prior to en-

129. *See* from the old English case law: Carlill v. Carbolic Smoke Ball Company [1893] 1 QB 256 (Eng.); Household Fire & Carriage Accident Ins. Co. v. Grant [1879] 4 Exch. Div. 216 (Eng.). On the German civil code: *Busche in Münchener Kommentar zum Bürgerlichen Gesetzbuch*, 7th ed. 2015, Vor §145 ¶ 31. On the French *Code Civil*: Cour de cassation [Cass.] [supreme court for judicial matters] com., Oct. 22, 1996, Bull. civ. IV, No. 261 (Fr.).

130. Even if we do not consider the validation nodes parties to the DL "contract," their conduct may matter if we include them as agents to the core group.

131. The legal basis for that may vary. In the U.K. or Australia, such conduct could give rise to remedies under statutory law. *See infra* Subsection III.D.2. In the U.S., an implied contract is likely to be found to exist. *See* Baltimore & Ohio R.R. v. United States, 261 U.S. 592, 597 (1923) (holding that "an agreement . . . is inferred, as a fact, from conduct of the parties showing, in the light of the surrounding circumstances, their tacit understanding.").

132. *See, e.g.*, BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], § 311, https://www.gesetze-im-internet.de/bgb/__311.html (Ger.) (not requiring consideration as a precondition for a "Schuldverhältnis" (best translated as "obligation")). Generally speaking, laws based on the Roman contract law do not insist on consideration as a precondition for obligations. *See, e.g.*, CODE CIVIL [C. CIV.] [CIVIL CODE] art. 1128 (Fr.) (listing as essential conditions for the validity of a contract: (1) agreement ("consentement des parties"), (2) ability ("capacité de contracter"), and (3) a legitimate and clear object ("contenu licite et certain")).

tering into the agreement, the greater the likelihood that judges will consider them as part of the contract. Warning language displayed prior to entering into the contract may constitute terms. Disclaimers and liability waivers may further limit obligations *if* they are upheld in court.[133] For contractual liability, however, it makes no difference whether the damage resulted from the misconduct of a human being or a machine's malfunction. The owner or operator is liable for the machine's malfunction.[134]

Contractual liability results in joint liability where the causes of action are not distinct and the defendants acted in furtherance of a common purpose.[135] Generally speaking, multiple nodes functioning together to run the ledger (hierarchy group two) and all core developers developing the code together (hierarchy group one) would meet that test on their respective hierarchy level. If nodes and developers cooperate, hierarchy groups one and two may find themselves tied together by joint liability *vis-à-vis* third parties.[136]

Some authors suggest that *no contractual relationship exists* in distributed networks where the user is unknown and the userbase unstable, where the performance of the service depends on who is connected at what time, and where none of the individual nodes is in itself essential (such as in permissionless blockchains like Bitcoin).[137] Proponents of the idea that the DLT relationship does not give rise to legal rights refer implicitly to participants' lack of intent to

133. General Public License or Open Source Software Licenses (OSSL) used by open source developers, including those that distributed the codes of Bitcoin and ETHER, use very broad language to limit liability. *See, e.g.*, *The MIT License*, OPEN SOURCE INITIATIVE, https://opensource.org/licenses/MIT (last visited May 16, 2018) ("THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE."). It is uncertain, however, whether courts will listen to this argument given that not a lot of courts have interpreted and applied the provisions of open source licenses. In particular, legislation in some countries provides for certain non-excludable warranties where a firm is carrying on a business. *See, e.g.*, U.C.C. §§ 2-314 to -316 (AM. LAW INST. & UNIF. LAW COMM'N 1977) (providing that certain warranties are implied in the sale of a product (as adopted by U.S. states)); *Competition and Consumer Act 2010* (Cth) sch 2 s 54(1) (Austl.) ("[T]here is a guarantee that the goods are of acceptable quality."). In light of such statutes, the exclusion clauses may not be effective in limiting liability for negligence and consequential damages. For the United States, see ROD DIXON, OPEN SOURCE SOFTWARE LAW 104–05 (2004) (stating that the exclusion of liability is void). For Australia, see Brian Fitzgerald & Nic Suzor, *Legal Issues for the Use of Free and Open Source Software in Government*, 29 MELB. U.L. REV. 412, 427–32 (2005) (arguing that the GPL liability exclusion will not withstand court scrutiny). For Germany, see TILL JAEGER & AXEL METZGER, OPEN SOURCE SOFTWARE 219, 224, 242, 266 (4th ed., 2016) (arguing that the exclusion of liability used in American open source licenses is null and void in certain cases due to violation of German legislation on prescribed contract terms; more generous exclusions can be agreed upon in arm's length negotiations).

134. For French law, see, *e.g.*, PHILIPPE MALAURIE, LAURENT AYNÈS & PHILIPPE STOFFEL-MUNCK, DROIT DES OBLIGATIONS 75 (2016).

135. For German law, BÜRGERLICHES GESETZBUCH [BGB] [Civil Code], § 421, *translation at* https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p1517 (Ger.).

136. This does not mean that groups 1 and 2 are liable toward each other or that end users necessarily have claims against the developers. On the discussion of waivers, see discussion at *supra* note 133.

137. Bayern, *supra* note 21, at 31–33; Dulong de Rosnay, *Peer-to-Peer*, *supra* note 24; Wright & De Filippi, *supra* note 110, at 55.

grant contractual rights to co-users.[138] Business entities, however, are often unaware of all participants, and their roles, in complex business interactions.[139] A distributed ledger is a complex network of users and contractual relationships that may change from time to time depending on who is participating in the ledger operation. While anonymity of the parties renders enforcement potentially difficult, it does not mean that the actions of individuals who together "operate" the distributed ledger are not legally relevant, potentially in a wide range of different jurisdictions.[140]

In a distributed ledger, electronic messages and transactions coincide; any message a node sends is a declaration of intent and contribution to the transaction.[141] It is inconsistent to deny legal relevance of cooperation where only reliance on others ensures access to, and transfer of,[142] one's own asset value and where this very cooperation by others is the precondition of contributing to the ledger in the first place. A simple example may demonstrate our point: Assume miners on the Bitcoin blockchain find, for whatever reason, that no one will accept (today) the newly- and properly-generated Bitcoins, or (after 21 million Bitcoins are mined) that people will accept the recycled Bitcoins, effectively creating a fork between the blockchain leading to this miner and all others. The miner who invested significant processing power (*i.e.*, energy) will either turn to the Bitcoin nodes that validate honestly mined coins (*i.e.*, all who hold Bitcoins directly)—for fulfilment of the promise given to them that honestly mined coins would become part of the chain, accepted by others as currency, and receive value—or to the core developers for damages. In both cases, the

138. Bayern, *supra* note 21, at 31–33 ("[A] bitcoin does not represent a transactional or organizational right in the way that shares of stock or a partnership interests do. . . . [G]iven merely my knowledge of a secret key for a certain amount of bitcoins, there is nobody associated with Bitcoin against whom I have a claim-right, and conversely nobody has a duty to me—apart from the general duty to refrain from interfering with intangible personal property. Those running the Bitcoin software are free to ignore my attempts to transfer bitcoins to a new bitcoin address. They have no contract with me, implied or otherwise. They are free to ignore me, to dispute my ownership of bitcoins on technological grounds, and so on. . . . In this sense, a bitcoin is not a right against the other users (*qua* users) of the Bitcoin network.").

139. This has prompted Teubner to analyze "networks as connected contracts." *See* TEUBNER, *supra* note 115, at 145–76; Gunther Teubner, *In the Blind Spot: The Hybridization of Contracting*, 8 THEORETICAL INQUIRIES L. 51, 51–52 (2006).

140. A number of legal questions follow from this statement, including: "When does liability start and end?" As a rule of thumb, if a node loses the ability to operate, it will drop out of the network, and thus liability.

141. This concept is inherent in automatized transactions. On smart contracts, see Koulu, *supra* note 110, at 61 ("[A] message is a transaction, a transaction is a message. . . . By making the transaction, each party enters into a contract."). *See also id.* at 65 ("[T]he declaration of intent is given through a transaction to the contract itself.").

142. Note that the person who sends the message to be incorporated into the blockchain is not the person who wants to receive a bitcoin but the person who wants to relinquish it. *See, e.g.*, SVERIGES RIKSBANK, FINANCIAL INFRASTRUCTURE REPORT 17 (2016), http://archive.riksbank.se/Documents/Rapporter/Fin_infra/2016/rap_finansiell_infrastruktur_160426_eng.pdf ("A transaction starts with a party that wishes to execute a payment, for instance, proposing the transaction to the network by sending a transaction instruction to the computers included in the network. Each participant in the network has a unique pair of keys that are used for encryption and it is through these that the participant can be identified in a secure manner. . . . The network checks that the transaction information is correct, for example that the recipient exists and that the sender owns the asset to which the transaction refers.").

miner has standing to sue based on the promise received by all Bitcoin nodes together, regardless of the fact that the miner did not, at the time, know the nodes or the developers. While enforcement may be difficult,[143] we must not confuse potential for legal liability with the challenge of *enforcement*.

Another argument against contractual liability is that node operators may have no way of knowing to which use their fragmented contribution to the network is put,[144] which, for instance, could include money laundering or terrorist financing. Again, this argument is flawed. Nodes *could* require AML/CFT ("Anti-Money Laundering/Combating the Financing of Terrorism") checks as a precondition for hard currency being exchanged into virtual assets—they could define this as a precondition for the overall use of the networks. The fact that nodes sign up to the network, particularly when they buy/sell/mine Bitcoins, without AML/CFT checks may evidence ignorance of the law but not the law's inapplicability.

2. Law of Torts: Delict and Special Liability Statutes

Joint tortfeasors are two or more individuals with joint and several liability in tort for the same injury to the same person or property.[145] Joint and several liability means the plaintiffs can collect any damages award from any one of a group of joint tortfeasors.[146] Tort claims are particularly important where there is no contractual liability, especially regarding DLT hierarchy group five suing the other DLT hierarchies, or in the case of DLT hierarchy groups one and two being sued by DLT hierarchy groups three and four in the absence of a contract.[147]

While the importance of these claims varies across jurisdictions, in many common and German-law-based civil law jurisdictions, the courts are loathe to award damages in tort for pure economic loss—the type of loss to which most risks will give rise. On the one hand, tort claims could arise from damages to "property" via the distributed ledger. The relevance of property-related claims

143. The miner would turn to the nodes it can identify and ask them to pay damages. *See* Dulong de Rosnay, *Peer-to-Peer*, *supra* note 24, Section 3.2 (suggesting collective insurance to mitigate the impact, but going on to argue that "collective intentionality" would lack legal personality).

144. *Id.* (drawing the conclusion that "it is questionable whether joint commitment or responsibility or contract may be applicable and helpful notions in the quest of distributed legal persons, rights or duties."); Wright & De Filippi, *supra* note 110, at 55–56.

145. For Germany, see BURGERLICHES GESETZBUCH [BGB] [CIVIL CODE], §§ 830, 840, *translation at* https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p0439 (Ger.). For France, see CODE CIVIL [C. CIV.] [CIVIL CODE] art. 1384(1) (Fr.). See also the French case, Cour de cassation [Cass.] [supreme court for judicial matters] 2e civ., Jul. 2, 1969, Bull. civ. II, No. 233 (Fr.).

146. *See id.*

147. *See* Primavera De Filippi, *Ethereum*, *in* ABÉCÉDAIRE DES ARCHITECTURES DISTRIBUÉES 100 (2015) (arguing in favor of tort claims against DAO developers); Francesca Musiani, Cécile Méadel, & Alexandre Mallard, *Bitcoin*, *in* ABÉCÉDAIRE DES ARCHITECTURES DISTRIBUÉES 45–46 (2015) (considering tort claims against Bitcoin code developers, while denying them against miners, nodes and owners of BTC); Wright & De Filippi, *supra* note 110, at 55–56 (arguing in favor of the developer's liability and against the user's liability since the user did not know, or did not have a good reason to believe, that the third party could potentially cause harm to someone).

depends on the legal qualification of the plaintiff's position in the system. For instance, if a Bitcoin is deemed tangible property,[148] intentional interference (*i.e.*, a hack or hard fork resulting in temporary denial of access or even permanent diversion of the Bitcoin owned by the user) could result in claims based on trespass to chattels or conversion,[149] but the application of tort law to Bitcoin as intangible property[150] is less certain.[151] On the other hand, claims could stem from fraud, theft, or other types of illicit conduct. Code modification could amount to any of the former.[152] Whether code modification in fact amounts to fraud or other types of actionable harm depends on, among other things, the user's intention. In most jurisdictions, intentionally inflicting harm on others results in liability for damages.[153]

An entity operating in the distributed ledger may be liable in tort if its negligent act, omission, or misstatement causes loss or damage, including loss due to a security breach or a coding error. A record on the system may be inaccurate, causing losses to those relying on it.[154] An entity's liability in negligence will depend on whether it owes a duty of care and has breached that duty, whether the breach caused loss or damage, and whether it has effectively contractually excluded liability for this type of loss or damage.[155]

The existence of a duty of care depends in part on the type of loss suffered and by whom it is suffered. In most potential distributed ledger actions, the rel-

148. Raskin, *supra* note 19, at 984–1005 (arguing that Bitcoin is tangible property for the purposes of civil procedure due to the exclusionary effect of the "owner's" access key and in favor of allocating jurisdiction based on rights *in rem*). Raskin's opinion is shared by the U.S. Internal Revenue Service. *See* I.R.S. Notice 2014-21, 2014-16 I.R.B. 938, http://www.irs.gov/irb/2014-16_IRB/ar12.html (arguing that virtual currency is property for tax purposes). *But see* Schroeder, *supra* note 17, at 14–27 (arguing that Bitcoin is not "money" under the U.S. Uniform Commercial Code since the Bitcoin owner lacks physical custody); *see also* Christopher, *supra* note 7, at 179–80.

149. On the U.S., see RESTATEMENT (SECOND) OF TORTS §§ 217, 218 (AM. LAW INST. 1965). On Australia, see *Penfolds Wines Proprietary Ltd v Elliott* (1946) 74 CLR 204, 216–19 (Austl.). On the UK, see Torts (Interference With Goods) Act 1977, c. 32, § 1 (UK).

150. *Cf.* Bayern, *supra* note 21, at 29–31 (stating that a Bitcoin is intangible personal property); Schroeder, *supra* note 17, at 23–42 (arguing that Bitcoin is a "general intangible" under the U.S. Uniform Commercial Code).

151. The answer partly depends on whether property doctrine such as trespass to chattel may be expanded into the electronic context. The case law and articles are too numerous to be discussed here in detail. For an overview from the U.S. perspective, see David M. Fritch, *Click Here for Lawsuit—Trespass to Chattels in Cyberspace*, 9 J. TECH. L. & POL'Y 31, 62–63 (2004); Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421, 421 (2002).

152. *But see* Bayern, *supra* note 21, at 33 n.28.

153. For the common law, *see id.* ("[I]nterference with individually owned bitcoins via a technological vulnerability on the owner's computer system probably amounts to conversion . . . ."). On German civil law, see BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], §1295, ¶ 2 (granting damages for pure economic loss). For French civil law, see CODE CIVIL [C. CIV.] [CIVIL CODE] art. 1382, 1383 (Fr.); Edward A. Tomlinson, *Tort Liability in France for the Act of Things: A Study of Judicial Lawmaking*, 48 LA. L. REV. 1299, 1314 (1988) ("These articles, everyone agreed, imposed liability only when the plaintiff established that the defendant's intentional (article 1382) or negligent (article 1383) wrongdoing caused the plaintiff's injury.").

154. *See* Vernon Valentine Palmer, *A Comparative Law Sketch of Pure Economic Loss*, *in* COMPARATIVE TORT LAW: GLOBAL PERSPECTIVES 300, 305–06 (Mauro Bussani & Anthony J. Sebok eds., 2015) (discussing potential liability for flawed data on which other parties rely).

155. *Id.* at 313 n.39.

evant loss is likely to be "pure economic loss" (*i.e.,* economic loss occurring in the absence of, or prior to, any damage to property or person).[156] Courts in common law countries (and many civil law countries) have been reluctant to find that a duty of care exists in cases of pure economic loss for fear of "imposing unreasonable burdens on the freedom of individuals to protect or pursue their own legitimate social and business interests . . . ."[157] One may be liable in negligence for pure economic loss in certain situations, however, especially if the plaintiff was a member of a class exposed to foreseeable loss by the defendant's conduct whose members were ascertainable by the defendant and if imposing the duty does not unreasonably interfere with the defendant's commercial freedom.[158] Some common law countries also have statutory provisions that extend the duty of care to apply in cases of pure economic loss. For example, in Australia's New South Wales, the Civil Liability Act of 2002 includes "economic loss" in the definition of "harm," and a person may be negligent in failing to take precautions against a risk of harm if the risk was foreseeable and not insignificant and a reasonable person in the person's position would have taken those precautions.[159]

The relevant operator might establish that no duty of care existed, particularly if the plaintiff is a second- or third-line victim and not part of an ascertainable class. Liability for pure economic loss is therefore more likely in the case of smaller, permission-based blockchains where the class of plaintiffs is readily ascertainable, although the plaintiff would still need to prove the entity breached its duty of care (by, for instance, not meeting the standard of a reasonable node or software developer) and that this breach caused the plaintiff's loss.[160] Operators may contractually exclude liability for negligence in these situations. Such an exclusion clause may be void, however, under consumer legislation or subject to narrow construction by the courts.

Over time, and painfully slowly from the perspective of technical innovation, courts in jurisdictions that allow tort claims for pure economic loss will shape the duties of care in the DLT context as distributed ledgers gain importance in business. This could result, for instance, in judicial pronouncements regarding the appropriate announcement time and method for code modifications, the required bit size and node computing power for the modification, and the necessary diligence prior to the new code's release.[161] In a way, the strictest

156. *Id.* at 311.

157. *Perre v Apand Proprietary Ltd* (1999) 198 CLR 180, 218 (Austl.); *also see id.* at 315.

158. *Id.* at 204.

159. *See, e.g.*, *Civil Liability Act 2002* (NSW) ss 3, 5B(1) (Austl.).

160. *See* John C. P. Goldberg & Benjamin C. Zipursky, *Torts as Wrongs*, 88 TEX. L. REV. 917, 958 (2010).

161. We do not share the generic view stated by Bayern, *supra* note 21, at 33 n.28 (arguing that Bitcoin owners reasonably intend to take the risk associated with further evolution of the Bitcoin computer system). Bitcoin has moved beyond an assembly of anarchic code developers into the commercial sphere. To the same extent as this development has amended the economic importance of Bitcoin, ledger participants must take into account the reasonable expectations of other participants when developing the code further. Material changes in code development, such as increasing the number, or speed, of Bitcoins to be mined could violate the developers' duty of care.

jurisdiction involved may determine the level of care for the whole ledger as lawsuits will be filed there. The important point here is, again, that groups one to four in our DLT hierarchy cannot act as they wish; rather, they need to keep the reasonable expectations of all parties relying on the respective ledger as well as the evolving case law in all jurisdictions where system users and beneficiaries can establish a court's jurisdiction[162] in mind, and risk liability if they do not.

162. As to jurisdiction, see discussions *infra* Subsection III.C.2 and Part V.

3. General Partnership or Joint Venture

The criteria of partnership law as to when a group of joint actors will be a partnership differ from jurisdiction to jurisdiction. While under the laws of some jurisdictions[163] the *joint pursuit of a (joint) objective* suffices to establish an unincorporated company,[164] the law of most common law jurisdictions requires the sharing of profits for a general partnership. If a cooperation is a partnership, it will usually result in joint liability.

For instance, while participation in a clearing and settlement distributed ledger system that relies on all nodes' mutual cooperation for identifying true transactions may be deemed a joint pursuit of a shared objective sufficient under some civil laws to establish a joint venture,[165] the fee and profit-sharing agreement will determine whether such a blockchain is deemed a partnership under common law. As long as profit opportunities are held by a third-party distributed ledger sponsor/organizer and the nodes bear their own expenses and are rewarded on a predetermined basis as with Bitcoin, the risk that the system is a partnership at common law is very low indeed.[166] If in a permissioned blockchain, however, the network of validation nodes offers the services of the network to third-party users which pay "the network" for these services, the system may be deemed a partnership; and in turn, all validation nodes as partners may be liable *vis-à-vis* third parties.

While the former shows that there is significant liability risk, the case of the DAO illustrates the potential magnitude of the risk. In the DAO, all investors jointly voted on investment proposals, all investors jointly held the assets acquired, no legal entity was positioned as a liability shield in between assets and investors, and all investors agreed that they were to share the profits gener-

163. Notably, German law on the Gesellschaft bürgerlichen Rechts ("unincorporated company"). In particular, it has been held that certain developer associations in the open source domain, such as the Apache Software Foundation, or core developer groups qualify as unincorporated companies if, in addition to the joint purpose of further developing an open source software, there is some, albeit purely factual, organizational structure. *See* JAEGER & METZGER, *supra* note 133, ¶¶ 193–200. The same applies to Blockchain core developer groups surrounding Bitcoin and Ethereum, in particular the Bitcoin foundation.

164. For instance, see BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE] § 705 (Ger.); CODE CIVIL [C. CIV.] [CIVIL CODE] art. 1832, 1833 (Fr.). Absent specific stipulations, the French law assumes that both profits and liability are to be distributed according to the size of the contribution of every partner. Further, under article 1833, a partnership's object has to be legitimate and in the partners' interest. In the case of a partnership (société de personnes) the *intuitu personæ* is determinative, meaning that the contract can be declared void in case of an error concerning the qualities or capacities of a putative partner, as ruled by the Cour de Cassation. Cour de Cassation [Cass.] [supreme court for judicial matters] com., Mar. 8, 1965, Bull. civ. III, No. 451.

165. An example could be provided by the Swiss giro network case, Bundesgericht [BGer] [Federal Supreme Court] June 27, 1995, 121 ENTSCHEIDUNGEN DES SCHWEIZERISCHEN BUNDESGERICHTS [BGE] III 310, 314–15 (Switz.), where the Swiss Federal Supreme Court has taken the view that, for purposes of external liability, the network should not be regarded as a collection of bilateral contracts but as a multilateral co-operative system similar to an unincorporated business organization; the argument rests on the ground that one bank could not meet its obligation without the other, so co-operation was an implicit condition of the contract. On the common law perspective, see Collins, *supra* note 114, at 64, 69 ("Such a radical departure from the ordinary principles of contractual responsibility seems unlikely to be imitated in the common law.").

166. Other features missing in permissionless systems may include the lack of a centralized coordinating authority that receives and distributes the residual profits.

ated by the assets. If the DAO's assets had generated losses rather than profits (for instance, if people working in a factory held by the DAO were harmed by an accident) all investors could be held to be partners and personally liable.[167]

As a rule of thumb, the risk of liability associated with DLT participation based on partnership law increases in the following circumstances:

1. the more a server owner benefits from participating in the distributed ledger through profits (as long as there are others who benefit in the same way);
2. the greater a server owner's influence is on the server design, set-up, or update, with "creators" being more influential than "simple users"; and
3. the greater the server owner's influence on the decision to let others use or be excluded from using the distributed ledger.

From the last consideration follows that the function of a validation node in a permissioned blockchain with a veto right[168] against access or updates (hereinafter called "consortium blockchain") is more likely to lead to personal liability than the "simple" mining function in Bitcoin. The result of the former may well not only be mutualization of data processing but also mutualization of liabilities and risks.

4. Specific Legislation, in Particular Competition Law

Regulators have suggested that DLT can pose a risk to fair competition and orderly markets. For example:

> ESMA anticipates . . . [e]arly [DLT] participants might refuse or impose conditions on new members that make it unduly difficult or costly for them to join the DLT network . . . . Also, it may become increasingly difficult to develop competing systems through time for cost or technical reasons, *e.g.*, patents that would protect certain components of the technology or the need to ensure interoperability with existing systems. This could drive some firms out of the market and lead to a monopoly-like situation with negative consequences on the cost and quality of the services.[169]

If DLT functions as a technological barrier that enables or facilitates monopolies, additional liability may stem from competition/antitrust law. This is of great importance since competition laws often impose antitrust liability on different criteria from contract or tort law. For instance, under European competi-

167. This view has been shared by Hinkes, *supra* note 17.

168. We refer to legal veto rights, rather than the option always existing in distributed ledgers to run a different code version than other nodes, and thereby hard fork the ledger.

169. *See* EUR. SEC. MKTS. AUTH., *supra* note 2, at 11, ¶ 37.

tion law, the definition of the responsible party may include the parent and subsidiary companies.[170]

While beyond the scope of this Article, market participants involved in a distributed ledger system must keep this and other conduct-related legislation (such as data protection,[171] copyright laws,[172] consumer-protection laws,[173] tax laws,[174] AML/CFT,[175] landlord-tenant laws,[176] etc.) in mind.

5. "Code-as-Law" Defense

Defendants in a lawsuit may raise the "code-as-law" defense. The argument (raised, for instance, by the hacker that captured the DAO's Ether[177]) is if code defines what is "law," anything possible under the coded design is "legal."

From a lawyer's perspective, the argument is weak. If someone writes code under which the person is entitled to steal others' money, the code will not legitimize theft. The power to make uniform rules is vested with the formal law-making bodies of the specific legal or governmental system: code is *not* law.

The original, unamended software design or a new software design that was the result of the agreed governance process,[178] however, may be considered *in a contractual claim* as a characteristic of the service or product. This is because contractual partners—in our DLT hierarchy groups one to four—have voluntarily chosen to use the code-based services and product as they are. For instance, in a proof-of-work consensus model, the fact that consensus building takes up to fifteen minutes is inherent to the model and not a breach of contract.

As a general matter, third parties—in our hierarchy group five—may or may not have accepted this DLT characteristic. If, for instance, a third party has

170. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 101, 102, 106, Oct. 26, 2012, 2012 O.J. (C 326) 1; W.P. Wils, *The Undertaking as Subject of E.C. Competition Law and the Imputation of Infringements to Natural or Legal Persons*, 25 EUR. L. REV. 99, 99–116 (2000); *see also* Pieter Van Cleynenbreugel, *Single Entity Tests in US Antitrust and EU Competition Law* 8 (Working Paper, June 21, 2011), https://ssrn.com/abstract=1889232 (discussing the EU-US differences). DLT may, however, also contribute to competition law compliance efficacy. *See* Ajinkya Mahesh Tulpule, *Enforcement and Compliance in a Blockchain(ed) World*, 1 CPI ANTITRUST CHRON. 45, 45 (2017).

171. LAW SOC'Y OF H.K., *supra* note 1, at 62; Matthias Berberich & Malgorzata Steiner, *Blockchain Technology and the GDPR—How to Reconcile Privacy and Distributed Ledgers?*, 2 EUR. DATA PROTECTION L. REV. 422, 422 (2016); Gabison, *supra* note 58, at 330–35.

172. Gabison, *supra* note 58, at 335–39.

173. On smart contracts, see Koulu, *supra* note 110, at 67.

174. Gruber, *supra* note 20, at 194.

175. Raskin, *supra* note 19, at 980–81.

176. Christopher, *supra* note 7, at 155 (arguing that access to an apartment governed by a blockchain may violate landlord-tenant laws if the blockchain inhibits the tenant's access following the tenant's default).

177. *See* Lester Coleman, *DAO Ether Hacker Warns Against Hard Fork*, CRYPTOCOINS NEWS (June 18, 2016, 5:55 PM), https://www.cryptocoinsnews.com/dao-ether-hacker-warns-hard-fork. *But see* LAW SOC'Y OF H.K., *supra* note 1, at 18–19.

178. For this reason, the DAO hacker's argument was flawed in two ways: First, code is not law; property, criminal, and other law apply. Second, under the DAO's governance arrangement, financial transactions were to be agreed on by all investors rather than one user (the hacker) alone.

standing under tort law, it may be able to recover for an unduly long closing time for a DLT-based transaction.

IV. IMPACT ON BLOCKCHAIN PARTICIPANTS

Given that there is liability risk to entities involved in or in contact with a DLT system, participants, as well as regulators, are well advised to take legal and technical precautions. What might these measures look like?

A. Participation as Operational Risk Contingent Liability

Centralized ledgers not only centralize processes, but also liability. Formerly, when looking at central counterparties, market participants not only paid for processing, but also for the risk cushion provided by one highly regulated and very solvent entity. Blockchain has the potential to mutualize control over these entities. Under legal principles all over the world, however, joint control is likely to come along with joint liability.

In light of the issues raised in previous sections, it would be inappropriate to treat potential liability risk as non-existent. In a non-technical sense, participation brings about a contingent liability that needs to be considered as part of the IT-based operational risk.

B. Provisioning Against Risk: Capital Requirements and Insurance

The Basel III capital adequacy rules, while recognizing information systems and IT importance, treat such risks as but one type of operational risk.[179] Under the Basel III Principles for Sound Management of Operational Risk:

> [M]anagement should ensure the bank has a sound technology infrastructure that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated and comprehensive risk management . . . . Management should make appropriate capital investment or otherwise provide for a robust infrastructure at all times, particularly before . . . new products are introduced.[180]

The Risk Management Principles lack further details.

179. *See* Vlasta Svatá & Martin Fleischmann, *IS/IT Risk Management in Banking Industry*, 2011 ACTA OECONOMICA PRAGENSIA 42, 42–60 (2011) (stating that current treatment of IS/IT-based risk is inadequate). To this day, the Basel risk management website has not devoted a special workflow to IS/IT risk. *See Basel Committee—Risk Management*, BANK FOR INT'L SETTLEMENTS, http://www.bis.org/list/bcbs/tid_50/index.htm (last visited May 16, 2018).

180. *See* BANK FOR INT'L SETTLEMENTS, BASEL COMM. ON BANKING SUPERVISION, PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK 15–16 (2011), http://www.bis.org/publ/bcbs195.pdf.

Under the Basel III standard, banks must hold capital against operational risk based on the income generated in the last reference period.[181] Under the advanced measurement approach ("AMA"), intermediaries must collect in a loss database for each incident: (1) the date of the loss event; (2) the date of its discovery; (3) the loss that was related to it; and (4) whether that loss was (fully or partially) recovered from insurance.[182] Then, the banks would be required to calculate the operational risk charge based on the historic data.

The Basel operational risk management framework is under revision; and under that revision, a clear link of operational risk management to a bank's technological processes is required.[183] Given the potentially large (even catastrophic) impact of losses, the frequency of events, and the intermediary's collection of all risk-related events in few global databases,[184] recognition of DLT risk and a predetermined risk budget similar to that for participation in a syndicate or other types of joint ventures could well be the outcome.

Related concerns arise particularly in the context of systems which could be classified as financial infrastructure. Financial infrastructure attracts separate and additional requirements under guidelines from IOSCO and the Committee on Payment and Market Infrastructures ("CPMI") of the Bank for International Settlements ("BIS").[185] The CPMI principles contain detailed requirements in terms of capital, risk management, etc., which would clearly apply in the context of DLT-based payment and securities settlement systems.

Even in the absence of capital adequacy rules, given that losses from DLT participation can be serious enough and sufficiently likely to be considered by top management, a financial intermediary's management could be required to establish a DLT-related risk budget, enter into insurance, or limit DLT participation to very large and established counterparties. Be this as it may, DLT participation does not come for free and requires consideration of each function in the DLT hierarchy and whether it adds to, or reduces, liability risk.

C. Distributed Ledger-Concentrated Ownership?

Liability matters little for a private party (an individual) with few assets who is therefore unlikely to become the target of a lawsuit (with anarchic code

181. *See* BANK FOR INT'L SETTLEMENTS, BASEL COMM. ON BANKING SUPERVISION, STANDARDISED MEASUREMENT APPROACH FOR OPERATIONAL RISK 9 (2016), http://www.bis.org/bcbs/publ/d355.pdf [hereinafter BASEL COMM. ON BANKING SUPERVISION, FOR OPERATIONAL RISK].

182. Notably, the risk framework dating back to Basel 2 (prior to the GFC) does not mention IS/IT risk as separate event types but looks at the results, including business disruption and failed execution. *See* BANK FOR INT'L SETTLEMENTS, BASEL COMM. ON BANKING SUPERVISION, INTERNATIONAL CONVERGENCE OF CAPITAL MEASUREMENT AND CAPITAL STANDARDS Annex 9 (2004), https://www.bis.org/publ/bcbs107.pdf.

183. *See* BASEL COMM. ON BANKING SUPERVISION, FOR OPERATIONAL RISK, *supra* note 181.

184. Marco Folpmers, *Basel's New Approach to Operational Risk: A Step Backwards*, GLOBAL ASS'N RISK PROFS., (Apr. 22, 2016), http://www.garp.org/#!/risk-intelligence/all/all/a1Z40000003CA7oEAG/basels-new-approach-operational-risk ("Since banks struggle with the collection of sufficient loss data, consortia (such as ORX) have arisen in which banks pool operational loss data.").

185. *Principles for Financial Market Infrastructures*, BANK FOR INT'L SETTLEMENTS, http://www.bis.org/cpmi/info_pfmi.htm (last visited May 16, 2018).

developers being an eminent example). Legal uncertainty, ambiguity, and lack of assets can function as a liability shield for individuals as the reward will not justify the costs of enforcement. The perspective of a globally operating financial or production conglomerate is different: those entities are likely targets of lawsuits, regardless of the little legal certainty provided by legislation and case law. This could lead to risk multiplication given that someone may test the waters, thereby influencing the set-up of any distributed ledger and potentially limiting the use cases of DLT. Given the international dimension, the legal assessment necessary to provide a full view of liability risk includes the laws of multiple jurisdictions. This is particularly true of a permissionless blockchain. All of this together turns the drafting (including choice of law provisions) of access terms, and decisions while part of the system, into complex and costly endeavors.

Both liability exposure and transaction costs for its assessment have implications for the ideal *legal* set-up of a DLT structure. As such, we may observe that the ideal setting could—ironically—take the form of a concentrated legal structure in a distributed ledger system.

Concentration may be achieved by two means. First, participation in the distributed ledger may be limited to controlled entities of a conglomerate. If, for instance, a large multinational bank, tech enterprise or financial market infrastructure operator *and its subsidiaries* set up a system, the desirable tech characteristic of additional trust may be achieved while liability risk is low. Second, multiple parties jointly interested in one service could leave the set-up and operation of the system to one global enterprise sufficiently large and capitalized to bear liability risk and acquire those services on a fee basis,[186] or they could set up and capitalize such an entity as a joint venture themselves. In this case, their role could be that of simple users, related service providers, or in some cases, independent third parties (comparing with DLT hierarchy groups three to five). Be this as it may, liability is a factor in structuring distributed ledger transactions that needs to be considered in the existing legal and regulatory framework and which may well lead to concentrated ownership in distributed ledgers.

V. LAW AS A FACTOR IN DLT STRUCTURING

The claim that risk vanishes simply due to the use of a blockchain is, from a legal perspective, ridiculous.

Our analysis of the laws of the most important legal systems has revealed four general principles related to liability. First, the more the ledger is organized or based on a predetermined governance structure (most evident in permissioned ledgers), the greater the risk that participants, particularly those participants that are influential and "control" the ledger, will be held liable for breach of contract or as partners of the "ledger partnership."

186. This seems to be the business model of IBM. Please note that an actor's liability risk is not affected by outsourcing. Hence, if the DL set-up and operation is deemed an outsourcing, liability will remain.

Second, cooperation of sophisticated financial and business services requires organization, and if the resource dealt with by the ledger is essential, investors will demand control rights in return for their investment. Common sense and economic need will push for permissioned ledgers, so liability will be a major factor. Large-scale economic use of the ledger will come with potential liability.

Third, permissionless ledgers are not the answer to the liability issue. Even in permissionless ledgers (such as Bitcoin), the liability risk is not zero but rather highly case specific. There is a strong differentiation of treatment among countries and low levels of legal certainty. These differences and uncertainties would result in higher legal costs and risk premia, especially for transnational permissionless systems.

Fourth, our thesis that liability matters in the establishment of distributed ledgers holds nothwithstanding the fact that the legal basis for liability will vary across jurisdictions. Some liability will arise from contract or liability statutes, some from special legislation, and some from tort or partnership law, but the net result of the joint, coordinated activity will most often be joint liability. From the perspective of globally active financial institutions and multinational enterprises, that there are many ways in which liability can result makes it legally far more difficult to enter into distributed ledgers across countries and with other firms. The *risk of entangling one's own balance sheet* with *other ledger parties' obligations* is a serious barrier to cross-firm ledgers.

Firms will try to mitigate these risks with choice of law and jurisdiction clauses, but this approach will be less effective with statutory, tortious, and partnership liability and with services offered to consumers (given the mandatory jurisdiction and applicable law typically associated with consumer transactions). Parties will choose the governing law to minimize liability, but liability risk may well harm, in particular, the development of cross-border ledger systems with many nodes.

The risk of distributed liability of distributed ledgers suggests that concentrated ownership is the most likely way of legally structuring distributed ledgers. Distributed ownership may be conditioned on a higher degree of legal certainty and a greater degree of harmonization across jurisdictions. Harmonization of private law consequences of DLT systems could be most useful, although this will of course be a long-term undertaking.[187] In addition, international regulatory cooperation in development of minimum regulatory standards will be key to addressing potential risks, and this begins with the technical harmonization presently underway.[188]

187. *See* Paech, *supra* note 17, at 1106–07 (examining options available under private international law to allocate blockchain arrangements across jurisdictions).

188. The International Organization for Standardization (ISO) has established a new technical committee to work on the harmonization of standards for blockchain and DLT, with Australia as the chair. *See ISO/TC 307: Blockchain and Distributed Ledger Technologies*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/committee/6266604.html (last visited May 16, 2018).

From a legal and regulatory perspective, the starting point must be to focus on the sorts of issues that will arise when any of the core attributes which make DLT systems attractive—namely their security, immutability, and transparency—fail, as fail they will. While DLT systems may be very secure from a technological perspective (at least those which are properly designed and built), from a legal perspective, they may well spread risk that was formerly concentrated in very few parties (or perhaps one party) across all system participants (nodes). With the realization that the failure of a distributed ledger system represents a risk, financial institutions will have to adjust their business strategies to accommodate the contingent liability involved in DLT. From the standpoint of immutability, once an error is embedded in the blockchain, this may be highly problematic, legally, in that law often requires the ability to rectify errors as a matter of law in a way foreign to DLT.[189] Instead of rectification, plaintiffs may turn to compensation. Likewise, transparency requires careful consideration in design to avoid liability for inadequate data protection.

As a result, DLT will have different impacts than many expect. In particular, liability will not be eliminated but may instead be spread across the system, and financial intermediaries involved in a distributed ledger should arguably hold capital or acquire insurance for contingent liabilities stemming from DLT participation. Likewise, operators may, in time, need to be governed by regulatory requirements similar to those governing other providers of systemically important infrastructure, such as traditional centralized payment and settlement systems.

Part of the thrill of blockchain to date has been its disregard of the law. With law in the picture, data are less attractively housed in distributed ledgers. This does not mean liability will exist in all cases. Liability matters, however, and distributed ledgers may, in time, most often be legally structured (particularly in permissioned systems) as a joint venture where all servers are owned and operated—ironically—by one entity, or a small number of specified entities, rather than as a cooperation among multiple entities.

189. *See* Paech, *supra* note 17, at 1097–98.