INTERNATIONAL BLOCKCHAIN REGULATION:

REGULATION BY CODE – OUTLAWS OR NEW CONCEPTIONS OF LAW?

Mona Flink
Master's Thesis
Advanced International Law and Technology
University of Turku
Faculty of Law
April 2021

Abstract

UNIVERSITY OF TURKU
Faculty of Law

MONA FLINK: International Blockchain Regulation: Regulation by Code – Outlaws or New Conceptions of Law?

Master's thesis, 69 p.

International Law

April 2021

Blockchain technology and globalization have challenged the dynamics of governments as regulators, the sovereignty of nation states, and understanding of jurisdiction. The role of private transnational actors has increased in the globalized world, and they have the power to influence human behavior and cause effects similar to positive law. The separate nature of cyberspace has generated jurisdictional discussions of cyberspace and whether cyberspace should form its own legal system with separate laws applicable. Technological change is rapid, and the development of international regulation has been lagging behind. Another regulatory challenge with blockchain technology is that it is based on network communication and has developed communities of private actors participating in the network. The need for international regulatory harmonization is recognized while it must be considered if traditional governance models are even optimal for blockchain technology.

This research analyzes jurisdictional premises and the limitations that blockchain technology that is occurring in cyberspace has posed to traditional jurisdictional concepts. The central part of the jurisdictional discussions is the concept of cyberspace jurisdiction and the frameworks of Lex Informatica, Lex Cryptographia, and Code is Law. After jurisdictional analysis, the current state of international blockchain regulation is analyzed with a new framework developed for blockchain technology and an existing one in order to resolve if current regulation could be adopted to blockchain technology. The research has a de lege ferenda approach with regulatory governance, and the regulatory governance solutions for blockchain technology will be analyzed.

The theoretical background of the research is critical technological determinism, and the key references are articles from legal journals and the principles of public international law. The summarized findings of this research are that the jurisdictional framework features technological determinism, and the possibilities of existing tools of international law to solve jurisdictional issues are overlooked. However, the role of transnational private actors is relevant for the development of blockchain regulation, and traditional government-oriented governance methods may not be optimal solutions for blockchain technology.

Keywords: International blockchain regulation, Blockchain, Jurisdiction, Cyberspace jurisdiction, Regulation, Governance, Technological determinism

Tiivistelmä

TURUN YLIOPSITO
Oikeustieteellinen tiedekunta

MONA FLINK: International Blockchain Regulation: Regulation by Code – Outlaws or New Conceptions of Law?

Pro gradu -tutkielma, 69 s.

Kansainvälinen oikeus

Huhtikuu 2021

Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisuus on tarkastettu Turnitin Originality Check -järjestelmällä.

Lohkoketjuteknologia ja globalisaatio ovat haastaneet hallitusten asemaa sääntelyviranomaisina, valtioiden suvereniteettia ja ymmärrystä lainkäyttövallasta. Yksityisten monikansallisten toimijoiden asema on kasvanut globaalissa maailmassa, ja heillä on kyky vaikuttaa ihmisten käyttäytymiseen luoden positiivisen oikeuden kaltaisia vaikutuksia. Kyberavaruuden erillisyys on saanut aikaan kyberavaruuden lainkäyttövaltaan liittyviä keskusteluja sekä sen, kuuluisiko kyberavaruuden muodostaa oma oikeusjärjestelmänsä, johon pätee erilliset sovellettavat lait. Teknologian muutos on nopeaa, ja kansainvälisen lainsäädännön kehitys on laahannut perässä. Lisäksi lohkoketjuteknologiaan liittyvä lainsäädännöllinen haaste on se, että lohkoketju perustuu tietoverkon kommunikaatioon ja se on perustanut yksityisiä yhteisöjä teknologian ympärille. Tarve kansainvälisen sääntelyn harmonisoinnille on tunnistettu, mutta samaan aikaan on harkittava soveltuvatko perinteiset hallintomallit optimaalisimmalla tavalla lohkoketjuteknologialle.

Tämä tutkimus analysoi lainkäyttövallan perusteita ja niitä rajoitteita, joita kyberavaruudessa toimiva lohkoketjuteknologia on aiheuttanut perinteisille lainkäyttövallan käsitteille. Keskeinen osa lainkäyttövallan analyysia on kyberavaruuden lainkäyttövallan käsite ja Lex Informatica, Lex Cryptographia ja Code is Law -viitekehykset. Lainkäyttövallan analyysin jälkeen lohkoketjuteknologian kansainvälisen sääntelyn tila analysoidaan uuden lohkoketjuteknologialle luodun viitekehyksen sekä olemassa olevan viitekehyksen avulla, jonka avulla selvitetään, voidaanko nykyistä lainsäädäntöä hyödyntää lohkoketjuteknologialle. Tällä tutkimuksella on de lege ferenda -lähestyminen lainsäädännön hallintotapaan, ja hallintotaparatkaisut lohkoketjuteknologialle ovat osa analyysia.

Tutkimuksen teoreettinen tausta on kriittinen teknologinen determinismi. Keskeiset lähteet ovat oikeustieteellisissä lehdissä julkaistut artikkelit sekä kansainvälisen oikeuden periaatteet. Tiivistetysti tutkimuksen loppupäätelminä voidaan todeta, että lainkäyttövallan viitekehykset ilmentävät teknologista determinismiä ja voimassa olevan kansainvälisen oikeuden mahdollisuudet ratkaista lainkäyttövaltaan liittyviä ongelmia on sivuutettu. Kuitenkin on syytä huomioida, että monikansallisten yksityisten tahojen rooli on merkityksellinen kehitettäessä lohkoketjusääntelyä ja perinteiset hallituskeskittyneet hallintomallit eivät välttämättä ole kaikista optimaalisimpia ratkaisuja lohkoketjuteknologialle.

Asiasanat: Kansainvälinen lohkoketjusääntely, Lohkoketju, Lainkäyttövalta, Kyberavaruuden lainkäyttövalta, Lainsäädäntö, Hallinto, Teknologinen determinismi

Table of Contents

REFERENCES

Literature

Allen, Hillary J.: Regulatory Sandboxes. George Washington Law Review 87 (3) 2019, pp. 579–645.

Atzori, Marcella: Blockchain Technology and Decentralized Governance: Is the State Still Necessary? Journal of Governance and Regulation, 6 (1) 2017, pp.45–62.

Balleste, Roy – Kulesza, Joanna: Signs and Portents in Cyberspace: The Rise of Jus Internet as a New Order in International Law. Fordham Intellectual Property, Media and Entertainment Law Journal 23 (4) 2013, pp. 1311–1349.

Bayón, Pablo: Key Legal Issues Surrounding Smart Contract Applications. KLRI Journal of Law and Legislation 9 (1) 2019, pp. 63–92.

Beck, Roman: Beyond Bitcoin: The Rise of Blockchain World. Computer 51 (2) 2018, pp. 54–58.

Behrens, Peter: The Extraterritorial Reach of EU Competition Law Revisited – The "effects doctrine" before the ECJ. Institute for European Integration, Discussion Paper 3/15 2016, pp.1–15.

Better Regulation Task Force: Routes to Better Regulation, A guide to alternatives to classic regulation. A Study Report on better regulation in the EU 2005.

Berg, Alastair – Markey-Towler, Brendan – Novak, Mikayla: Blockchains: Less Government, More Market. The Journal of Private Enterprise 35 (2) 2020, pp. 1–21.

Black, Julia: Decentering Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World. Current Legal Problems 54 (1) 2001, pp. 103–146.

Borg, Joseph F. – Schembri, Tessa: Blockchain & Cryptocurrency Regulation. 1st ed., Global Legal Group Ltd. 2018.

Bratspies, Rebecca M.: Cryptocurrency and the Myth of the Trustless Transaction. Michigan Technology Law Review 25 (1) 2018, pp. 1–57.

Brownlie, Ian: Principles of Public International Law. 7th ed., Oxford University Press 2008.

Butenko, Anna – Larouche, Pierre: Regulation for Innovativeness or Regulation of Innovation? TILEC Discussion Paper, March 2015.

Calliess, Gralf-Peter: Reflexive Transnational Law: The Privatization of Civil Law and the Civilization of Private Law. The German Journal of Law and Society 23 2002, pp. 185–216.

Calliess, Gralf-Peter – Zumbansen, Peer: Rough Consensus and Running Code a Theory of Transnational Private Law. Bloomsbury Publishing Plc 2012.

Catá Backer, Larry: Multinational Corporations as Objects and Sources of Transnational Regulation. ILSA Journal of International & Comparative Law 14 (2) 2008, pp. 1–26.

Catá Backer, Larry: Private Actors and Public Governance Beyond the State: The Multinational Corporation, the Financial Stability Board, and the Global Governance Order. Indiana Journal of Global Legal Studies 18 (2) 2011, pp. 751–802.

Catá Backer, Larry: The Structural Characteristics of Global Law for the 21st Century: Fracture, Fluidity, Permeability, and Polycentricity. Tilburg Law Review 17 2012, pp. 177–199.

Cheung, Anne S. Y. – Weber, Rolf H.: Privacy and Legal Issues in Cloud Computing. Edwards Elgar Pub. Ltd. 2015.

Cockfield, Arthur J.: Towards a Law and Technology Theory. Manitoba Law Journal 30 (3) 2004, pp. 383–415.

Cohen, Harlan G.: Finding International Law: Rethinking the Doctrine of Sources. Iowa Law Review 93 (65) 2007, pp. 65–129.

Dafoe, Allan: On Technological Determinism: A Typology, Scope Conditions, and a Mechanism. Science, Technology & Human Values 40 (6) 2015, pp.1047–1076.

De Filippi, Primavera: Blockchain and the Law: The Rule of Code. Harvard University Press 2018.

De Filippi, Primavera – Loveluck, Benjamin: The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure. Internet Policy Review; Journal on Internet Regulation 5 (3) 2016, pp. 1–28.

Dimitropoulos, Georgios: The Law of Blockchain. Washington Law Review 95 (3) 2020, pp. 1117–92.

Dorsett, Shaunnagh – McVeigh, Shaun: Jurisdiction. Routledge 2012.

Drummer, Daniel – Neumann, Dirk: Is Code Law? Current Legal and Technical Adoption Issues and Remedies for Blockchain-Enabled Smart Contracts. Journal of Information Technology 8/2020.

Daluwathumullagamage, Dulani Jayasuriya – Sims, Alexandra: Blockchain-Enabled Corporate Governance and Regulation. International Journal of Financial Studies 8 (2) 2020, pp. 1–38.

European Union Blockchain Observatory & Forum: Legal and Regulatory Framework of Blockchains and Smart Contracts – Thematic Report. 27.9.2019.

Finck, Michèle: Blockchains: Regulating the Unknown. German Law Journal 19 (4) 2017, pp. 665–692.

Fishman, Donald A.: The Promise and Perils of Cyberlaw: Taking Communication Law Research to the Next Level. Free Speech Yearbook 37 1999, pp. 83–106.

Fosch Villaronga, Eduard – Golia, Angelo Jr: Robots, Standards and the Law: Rivalries Between Private Standards and Public Policymaking for Robot Governance. Computer Law & Security Review 35 2019, pp. 129–144.

Fyrigou-Koulouri: Blockchain Technology: An Interconnected Legal Framework for an Interconnected System. Journal of Law, Technology & the Internet Vol. 9 2018, pp. 1–14.

Gautier, Philippe: The Reparation for Injuries Case Revisited: The Personality of the European Union. Max Planck Yearbook of United Nations Law 4 2000, pp. 331–361.

Gikay, Asress: European Consumer Law and Blockchain based Financial Services: A Functional Approach against the Rhetoric of Regulatory Uncertainty. Tilburg Law Review 24 (1) 2019, pp. 27–48.

Gillespie, Tarleton: Engineering a Principle: 'End-to-End' in the Design of the Internet. Social Studies of Science 36 (3) 2006, pp. 427–457.

Girasa, Rosario: Regulation of Cryptocurrencies and Blockchain Technologies: National and International Perspectives. Palgrave Studies in Financial Services Technology 2018.

Global Financial Innovation Network (GFIN): Terms of Reference for Membership and Governance of the Global Financial Innovation Network (GFIN). 2019.

Goldsmith, Jack L.: Against Cyberanarchy. University of Chicago Law Review 65 (4) 1998, pp. 1199–1250.

Goldsmith, Jack – Wu, Tim: Who Controls the Internet?: Illusions of a Borderless World. Cary: Oxford University Press USA 2006.

Governatori, Guido – Idelberger, Florian – Milosevic, Zoran – Riveret, Regis – Sartor, Giovanni –Xu, Xiwei: On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain Systems. Artificial intelligence and law 26 (4) 2018, pp. 377–409.

Grant, John P. – Barker, Graig J. – Parry, Clive: Parry and Grant Encyclopaedic Dictionary of International Law. 3rd ed., Oxford University Press 2009.

Gunther, Teubner: Constitutional Fragments: Societal Constitutionalism and Globalization. Oxford University Press 2012.

Guzman, Andrew T.: Introduction - International Regulatory Harmonization. Chicago Journal of International Law, 3 (2), pp. 271-276.

Hassan, Samer – De Filippi, Primavera: The Expansion of Algorithmic Governance: From Code is Law to Law is Code. Field Actions Science Reports: The Journal of Field Actions 17/2017, pp. 88–90.

Hildebrandt, Mirelle: Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Edward Elgar Publishing 2015.

Hytha, David A. – Aronson, Jonathan D. – Eng, Al: Technology Innovation and the Rebirth of Self-Regulation: How the Internet of Things, Cloud Computing, Blockchain, and

Artificial Intelligence Solve Big Problems Managing Environmental Regulation and Resources. International Journal of Communication Vol. 13 2019, pp. 5568-5572.

International Bar Association (IBA): IBA Legal Policy & Research Unit Legal Paper, Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World. 2017.

International Chamber of Commerce: Rethinking Trade and Finance: An ICC Private Sector Development Perspective. ICC Publication No. 884E 2017.

International Panel on Social Progress: Report: Rethinking Society for the 21st Century. Cambridge University Press 2018.

Jansen, Bart: Towards a Hermeneutics of Pathetic Dots: Finding the Gap Between Law and Reality. Yuridika 34 (3) 2019, pp. 419–428.

Joerges, Christian – Sand, Inger-Johanne – Teubner, Gunther: Transnational Governance and Constitutionalism. Bloomsbury Publishing Plc 2004.

Johnson, David R. – Post, David: Law and Borders: The Rise of Law in Cyberspace. Stanford Law Review 48 (5) 1996, pp.1367–1402.

Jun, MyungSan: Blockchain Government - A Next Form of Infrastructure for the Twenty-First Century. Journal of Open Innovation 4 (1) 2018, pp. 1–12.

Karvonen, Erkki: Teknologinen determinismi. Tiedotustutkimus 22 (4) 1999, pp. 82–89.

Klabbers, Jan – Wallendahl, Åsa: Research Handbook on the Law of International Organizations. Edward Elgar Publishing 2011.

Ko, Haksoo: Law and Technology of Data Privacy: A Case for International Harmonization. Asian Journal of Law and Economics 3 (1) 2012, pp. 1–31.

Korhonen, Outi – Ala-Ruona, Jari: Regulating the Blockchain Society. Liikejuridiikka 3/2018.

Kuehl, Starr: From Cyberspace to Cyberpower: Defining the Problem. Potomac Books 2011.

Kulesza, Joanna: International Internet Law. Routledge 2012.

Laidlaw, Emily B.: A Framework for Identifying Internet Information Gatekeepers. International Review of Law, Computers & Technology 24 (3) 2010, pp. 263–276.

Leiser, Mark: The Problem with 'dots': Questioning the Role of Rationality in the Online Environment. International Review of Law, Computers & Technology 30 (3) 2016, pp. 191–210.

Lessig, Lawrence: Code: Version 2.0. Basic Books 2008.

Lessig, Lawrence: The Law of the Horse: What Cyberlaw Might Teach. Harvard Law Review 113 (2) 1999, pp. 501–549.

Lipton, Jacqueline: The Scope of Cyberlaw. In Rethinking Cyberlaw. Edward Elgar Publishing 2015, pp. 1–13.

Marchant, Gary E. – Abbott, Kenneth W.: International Harmonization of Nanotechnology Governance through Soft Law Approaches. Nanotechnology Law & Business 9 (4) 2013, pp. 393–410.

Mefford, Aron: Lex Informatica: Foundations of Law on the Internet. Indiana Journal of Global Legal Studies, 5 (1) 1997, pp. 211-238.

Melnyk, Roman – Barikova, Anna: Cross-Border Public Administration: Prospects for Introducing Blockchain Jurisdiction. Informatologia 52 2019, pp. 74–89.

Menthe, Darrel C.: Jurisdiction in Cyberspace: A Theory of International Spaces. Michigan Telecommunications and Technology Law Review 4 (1) 1998, pp. 69–103.

Mougayar, William – Buterin, Vitalik: The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. 1st ed. John Wiley & Sons 2016.

Murray, Andrew D.: Regulation and Rights in Networked Space. Journal of Law and Society 30 (2) 2003, pp. 187–216.

Murray, Andrew D.: Nodes and Gravity in Virtual Space. Legisprudence 5 (2) 2011, pp. 195–222.

Nakamoto, Satoshi: Peer-to-Peer Electronic Cash System. White Paper 2008.

OECD: International Regulatory Co-operation: The Role of International Organizations in Fostering Better Rules of Globalization. OECD Publishing 2016.

OECD: The OECD Report on Regulatory Reform: Synthesis. Paris 1997.

OECD: The Policy Environment for Blockchain Innovation and Adoption: 2019 OECD Global Blockchain Policy Forum Summary Report. OECD Blockchain Policy Series, 2019.

OECD Report: Alternatives to Traditional Regulation. 2002.

Orakhelashvili, Alexander: Research Handbook on Jurisdiction and Immunities in International Law. Edward Elgar Pub. Ltd 2015.

Reed, Chris: Online and Offline Equivalence: Aspirations and Achievement. International Journal of Law and Information Technology 18 (3) 2010, pp. 248–273.

Reidenberg, Joel R.: Lex Informatica: The Formulation of Information Policy Rules through Technology. Texas Law Review 76 (3) 1998, pp. 553–593.

Reidenberg, Joel R.: Technology and Internet Jurisdiction. University of Pennsylvania Law Review 153 (6) 2005, pp. 1951–1974.

Salmon, John – Myers, Gordon: Blockchain and Associated Legal Issues for Emerging Markets. International Finance Corporation, Washington, DC. 2019.

Singer, Joseph: The Player and the Cards: Nihilism and Legal Theory. The Yale Law Journal 94 (1) 1984, pp. 1–70.

Smith, Dimity Kingsford: Beyond the Rule of Law - Decentered Regulation in Online Investing. Law & Policy 26 (3–4) 2004, pp. 439-476.

Stone, Randall W.: Controlling Institutions: International Organizations and the Global Economy. Cambridge University Press 2011.

Sultan, Karim – Ruhi, Umar – Lakhani, Rubina: Conceptualizing Blockchains: Characteristics & Applications. 11th IADIS International Conference Information Systems 2018, pp. 49–57.

Swan, Melanie: Blockchain. O'Reilly Media, Inc 2015.

Takahashi, Koji: Implications of the Blockchain Technology for the UNCITRAL Works. UNCITRAL Modernizing International Trade Law to Support Innovation and Sustainable Development – Proceedings of the Congress of the United Nations Commission on International Trade Law. Volume 4: Papers presented at the Congress 2017, pp. 81–94.

Teubner, Gunther: Breaking Frames: The Global Interplay of Legal and Social Systems. The American Journal of Comparative Law, Vol 45 1997, pp. 149–208.

Thompson, Marcelo: The Neutralization of Harmony: The Problem of Technological Neutrality, East and West. Boston University Journal of Science & Technology Law 18 (2) 2012, pp. 303–342.

Tsagourias, Nikolaos K. – Buchan, Russel: Research Handbook on International Law and Cyberspace. Edward Elgar Pub. Ltd. 2015.

Twigg-Flesner, Christian: Disruptive Technology - Disrupted Law? How the Digital Revolution Affects (Contract) Law. In: Alberto De Franceschi (ed), European Contract Law and the Digital Single Market, Intersentia 2016.

Uerpmann-Wittzack, Robert: Principles of International Internet Law. German Law Journal 11(11) 2010, pp. 1245–1263.

United Nations: Yearbook of the International Law Commission Volume II, Documents of the Eighth Session Including the Report of the Commission to the General Assembly. United Nations Publication 1956.

Walch, Angela: The Path of The Blockchain Lexicon (and the Law). Review of Banking & Financial law, Vol 36 2016–2017, pp.713–765.

Walport, Mark: Distributed Ledger Technology: Beyond Block Chain, A Report by the UK Government Chief Scientific Adviser. December 2015.

Wang, Yu – Ren, Jing – Lim, Caroline – Lo, Swee-Won: A Review of Fast-growing Blockchain Hubs in Asia. The Journal of The British Blockchain Association 2 (2) 20219.

Weinstein, John – Cohn, Alan – Parker, Chelsea: Promoting Innovation Through Education: The Blockchain Industry, Law Enforcement and Regulators Work Towards a Common Goal. Global Legal Insights – Blockchain & Cryptocurrency Regulation, 1st ed., Global Legal Group Ltd 2018.

Werbach, Kevin: A Layered Model for Internet Policy. Journal of Telecommunications and High-Tech Law 37 2002, pp. 1–26.

Werbach, Kevin – Cornell, Nicolas: Contracts Ex Machina. Duke Law Journal 67 (2) 2017, pp. 313–382.

Windbichler, Christine: Lex Mercatoria. International Encyclopaedia of the Social & Behavioural Sciences, Vol 13 2015, pp. 915–918.

World Bank Group: Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives - Guidance Notes Series; Note 1: Collateral Registry, Secured Transactions Law and Practice. International Bank for Reconstruction and Development / The World Bank 2020.

Wright, Aaron – De Filippi, Primavera: Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Social Sciences Research Network 2015, pp. 1–58.

Zeros, Gerogios I.: State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction. International Journal of Law and Information Technology, 15 (1) 2007, pp. 1–37.

Zhang, Rui, Rui Xue, and Ling Liu: Security and Privacy on Blockchain. ACM Computing Surveys (CSUR) 52 (3) 2019, pp.1–34.

Ziolkowski, Rafael – Miscione, Gianluca – Schwabe, Gerhard: Decision Problems in Blockchain Governance: Old Wine in New Bottles or Walking in Someone Else's Shoes? Journal of Management Information Systems 37 (2) 2020, pp. 316–348.

Zumbansen, Peer: Transnational Private Regulatory Governance: Ambiguities of Public Authority and Private Power. Law and Contemporary Problems 76 (2) 2013, pp. 117–138.

Zwitter, Andrej – Hazenberg, Jilles: Decentralized Network Governance: Blockchain Technology and the Future of Regulation. Frontiers in Blockchain 3 (12) 2020, pp. 1–12.

Ølnes, Svein – Ubacht, Jolien – Janssen, Marijn: Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. Government Information Quarterly 34 (2) 2017, pp. 355–364.

Online sources

Barlow, John: A Declaration of the Independence of Cyberspace. 8.2.1996. (https://www.eff.org/cyberspace-independence) Accessed: 20.9.2020.

Brody, Paul: How Public Blockchains are Making Private Blockchains Obsolete. 6.12.2019. (https://www.ey.com/en_gl/consulting/whats-essential-to-scale-blockchain).

Business Insider Intelligence: The Growing List of Applications and Use Cases of Blockchain Technology in Business and Life. 2.3.2020. (https://www.businessinsider.com/blockchain-technology-applications-use-cases?r=US&IR=T) Accessed: 4.12.2020.

Cosset, Damien: Blockchain: What is Mining? DEV 5.1.2018. (https://dev.to/damcosset/blockchain-what-is-mining-2eod) Accessed: 15.11.2020.

European Commission: Legal and Regulatory Framework for Blockchain. 24.9.2020. (https://ec.europa.eu/digital-single-market/en/legal-and-regulatory-framework-blockchain) Accessed: 13.11.2020.

Forbes: The False Narrative of Bitcoin's Role in Illicit Activity. 19.1.2021. (https://www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/?sh=5be0d4623432) Accessed: 19.3.2021.

Hardt, Mortiz: How Big Data is Unfair: Understanding Unintended Sources of Unfairness in Data Driven Decision Making. 26.9.2014. (https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de) Accessed: 24.11.2020.

Information Technology and Innovation Foundation: A Policymaker's Guide to Blockchain. (https://itif.org/publications/2019/04/30/policymakers-guide-blockchain) Accessed: 23.11.2020.

ITU: ITU-T Recommendations. 2020a. (https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx). Accessed: 20.11.2020.

ITU: About International Telecommunication Union (ITU). 2020b. (https://www.itu.int/en/about/Pages/default.aspx) Accessed: 23.10.2020.

Kasireddy, Preethi: What Do We Mean by "Blockchains Are Trustless"?. 19.2.2018. (https://www.preethikasireddy.com/post/what-do-we-mean-by-blockchains-are-trustless#Story). Accessed 8.12.2020.

Ng, Irene: UNCITRAL E-Commerce Law 2.0: Blockchain and Smart Contracts. (https://lawtech.asia/uncitral-e-commerce-law/#_ftn6) Accessed: 27.11.2020.

Orcutt, Mike: A Crypto Project to Make Internet Names Censorship-proof is Now Live. MIT Technology Review, 7.2.2021. (https://www.technologyreview.com/2020/02/07/844900/handshake-network-dns-live/) Accessed: 8.3.2021.

Orcutt, Mike: Once Hailed as Unhackable, Blockchains are Now Getting Hacked. MIT Technology Review 19.2.2019. (https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/). Accessed: 8.3.2021.

PwC: PwC's Global Blockchain Survey. 2018. (https://www.pwc.com/gx/en/industries/technology/blockchain/blockchain-in-business.html) Accessed: 16.11.2020.

Roush, Wade: ICANN's Boondoggle: The Group that Oversees Internet Domain Names Is Shaking Things Up for No Good Reason. MIT Technology Review, 21.8.2021. (https://www.technologyreview.com/2012/08/21/184212/icanns-boondoggle/) Accessed: 8.3.2021.

Schneier, Bruce: Schneier on Security: Blockchain and Trust. 12.2.2019. (https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html) Accessed: 12.12.2020.

The Union of International Associations: Types of International Organization. 2021. (https://uia.org/archive/types-organization/cc) Accessed 1.2.2021.

United Nations Commission on International Trade Law: About UNCITRAL. 2020. (https://uncitral.un.org/en/about) Accessed: 6.11.2020.

Voshmigr, Shermin: Token Economy: How the Web3 Reinvents the Internet. 2020. (https://github.com/sherminvo/TokenEconomyBook/wiki/Governance-of-Web3-Networks-&-Other-DAOs) Accessed: 10.3.2020.

World Economic Forum: All You Need to Know about Blockchain, Explained Simply. 17.6.2016. (https://www.weforum.org/agenda/2016/06/blockchain-explained-simply/, Accessed 28 August 2020).

Official material

European Commission (COM): A European Agenda for the Collaborative Economy (2016)

The International Court of Justice: Reports of Judgments, Advisory Opinions and Orders. Advisory Opinion of April 11th, 1949.

The International Telecommunication Union (ITU-T): Telecommunication and Standardization of ITU, Technical Report FG DLT D4.1, Distributed Ledger Technology Regulatory Framework 1.8.2019.

OECD Council Recommendation on Principles for Internet Policy Making (2011)

OECD Principles of Corporate Governance (2004)

UNCITRAL Model Law on Electronic Commerce (1996)

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001)

UNCITRAL Convention on the Use of Electronic Communications in International Contracts (2005)

UNCITRAL Model Law on Electronic Transferable Records (2017)

UNCITRAL Model Law on Secured Transactions (2019)

The United Nations Convention on Law of the Sea (1982)

The United Nations Charter (1945)

The Vienna Convention on the Law of the Treaties between States and International Organizations or between International Organization (1986)

World Summit on the Information Society: Declaration of Principles, Building the Information Society: a global challenge in the new Millennium. Document WSIS-03/GENEVA/DOC/4-E 12.12.2003.

Case Law

The International Court of Justice:

Reparation for Injuries Suffered in the Service of the United Nations (1949)

US Court of Appeals for the Ninth Circuit:

AT&T vs City of Portland (2000)

Union des étudiants juifs de France:

Yahoo! INC. vs LICRA (2000)

Figures and tables

Figure 1: Laidlaw, Emily B.: A Framework for Identifying Internet Information Gatekeepers. International Review of Law, Computers & Technology 24 (3) 2010, pp. 263–276.

Figure 2: Lessig, Lawrence: Code: Version 2.0. Basic Books 2008.

Figure 4: Murray, Andrew D.: Nodes and Gravity in Virtual Space. Legisprudence 5 (2) 2011, pp. 195–222.

Table 1: Reidenberg, Joel.R: Lex Informatica: The Formulation of Information Policy Rules through Technology. Texas Law Review 76 (3) 1998, pp. 553–593.

Table 2: The International Telecommunication Union (ITU-T): Telecommunication and Standardization of ITU, Technical Report FG DLT D4.1, Distributed Ledger Technology Regulatory Framework 1.8.2019.

ABBREVIATIONS

CHMK	Common Heritage of Mankind
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technology
DNS	Domain Name System
GFIN	Global Financial Innovation Network
GDPR	General Data Protection Regulation
E2E	End-to-End
EU	European Union
IBA	International Bar Association
ICANN	The Internet Corporation for Assigned Names and Numbers
ICJ	The International Court of Justice
ICC	International Chamber of Commerce
IIG	Internet Information Gatekeeper
IIL	International Internet Law
IRC	International Regulatory Co-operation
ITIF	Information Technology and Innovation Foundation
ITU	International Telecommunication Union
ISP	Internet Service Provider
ML	Machine Learning
OSS	Open-Source Software
P2P	Peer-to-Peer
PCIJ	The Permanent Court of International Justice
SC	Smart Contract
UNCITRAL	The United Nations Commission on International Trade Law
UN	United Nations

1 INTRODUCTION

1.1 Background

"We have proposed a system for electronic transactions without relying on trust." [1]

The idea of blockchain technology was first presented by Satoshi Nakamoto in 2008 in his white paper "*Bitcoin: A Peer-to-Peer Electronic Cash System*". However, the term "blockchain" was not yet mentioned. Blockchain may be better known for the public from its applications such as Bitcoin and Ethereum rather than the technological features themselves.

It is frequently said in spoken language that technological development is continuous, and legislation is commonly a step behind. In addition to this, there exists a theoretical development of the jurisdictional framework of cyberspace[2] that could, according to techno-positivists, establish a separate legal system that is based on different rules than what we traditionally understand of legal systems.

The new conception of law refers to the aspect where technology, and blockchain, as an autonomous force, can influence societies and behavior. Could specific technologies such as blockchain establish an autonomous conception of law that can be compared to some extent with legal positivism? Legal positivism is highly associated with the validity of the law. The autonomous conception entails that shifts within society cannot affect the existence of law, which means that technology cannot change the mode of existence of the law or challenge its theoretical architecture. According to this understanding of law, it is assumed that most legal issues posed by online activity can be decided and solved within the existing legal framework, and if not, new laws should be passed, but this is a matter of politics.[3] However, even if technology would not be able to change the mode of existence of the law, it does not mean that it does not have effects similar to *positive law*. Another relevant aspect is the *de facto* effects technology, and blockchain, have on society and the behavior of individuals, whether it is or is not the law in the context of legal positivism.

[1] Nakamoto 2008, p. 8.
[2] The concept of cyberspace will be discussed in the following chapters.
[3] Hildebrandt 2015, p. 169.

The roles of private transnational actors have increased in the global world as well as their power to impact societies and human behavior. This has challenged the role of governments as regulators and the sovereignty of nation states. Instead of focusing on the two opposites, private and public, the focus is on the solutions on how these both can co-operate and co-exists optimally for better global governance. It must be noted that establishing a centered regulatory governance for blockchain technology may not be the optimal solution.

1.2 Brief Introduction to Blockchain Features

The technological features of blockchain have enabled new ways to organize matters which have previously belonged to a central authority, such as banks. In order to understand the jurisdictional and regulatory implications, it is essential to understand the central features of blockchain technology, which is why these will be briefly introduced.

For the sake of clarity of this research, it must be clarified that blockchain is based on the Distributed Ledger Technology (DLT). However, technologically they may not be identically equivalent to each other, but the purpose of this research is not to comment on the technological features specifically. In this research, the terms "blockchain", "blockchain technology" and "distributed ledger technology" refer all to blockchain.

In this regard, we understand how laws regulate, but to understand how codes "regulate" in the cyber world, we must have a basic understanding of how the software that formulates the cyber world also formulates the "regulation of code". [4] The key is to understand that a blockchain is a decentralized database or *a digital ledger* of transactions that is visible for all in the network. Basically, blockchain technology can work for nearly all types of transactions, including value such as money, property, and other goods.[5] All started with the launch of the cryptocurrency *Bitcoin* in 2009, but nowadays, in 2021, we are additionally talking about smart contracts, smart property, other cryptocurrencies such as Ethereum, supply chains, and public sector governance, for example.

The central elements for understanding (public) blockchains are (1) transactions occur in a peer-to-peer network, (2) there is no need for financial institutions or other third parties, (3) the

[4] Lessig 2008, p. 5. See also Reidenberg 1998, p. 568–573: Policy choices are available through technology itself; through laws that pose technology to exclude some options; or through laws that require users to restrict some actions (Lex Informatica).
[5] World Economic Forum, 2016.

transaction is proofed cryptographically instead of central trust, and (4) the trust is in the network instead of in a centralized institution.[6] Nevertheless, the concept of trust in a blockchain is debated in the literature and will be discussed later. *Technically* a blockchain is a database that maintains a distributed ledger openly, *businesswise* it is a network for moving value between parties or peers, and *legally* a blockchain is a mechanism for validating transactions not requiring middlemen.[7]

Every transaction forms its own block, which is attached to the chain of data blocks. The central elements on blockchains are *hashes* that secure the data storage of the blockchain and return a fingerprint that verifies the data authenticity.[8] The hash illustrates the exact content of the original file, and anytime the content must be reconfirmed, the hash runs an algorithm over the file and the data *fingerprint* will be the same in case the file has not changed. This consensus procedure is called *proof-of-stake*. The hashes are *timestamped*[9]*,* which proves that the data has existed at the time.[10] The protocol is that the computers in the network, called *nodes*, must verify a new transaction by comparing a new hash to the existing ones and thus confirm the existence of the transaction before it will be added into the database.[11]

Attempts to alter the information require rehashing not only the transaction-relevant block but all the succeeding blocks, in other words, the whole chain. Theoretically this is possible, but practically quite challenging since the chain is constantly growing as other nodes add new blocks to the chain of blocks.[12]

Blockchain technology introduces a series of characteristics that are novel in terms of transactions. Blockchains enable Decentralized Autonomous Organizations (DAO), which makes it possible for the participants to execute contracts and transactions without being their own legal entity. However, transactions can additionally be executed without DAOs. Transactions are transparent to DAO members, which is said to minimize fraudulent behavior.[13]

[6] Nakamoto 2008, pp. 2–3.
[7] Mougayar – Buterin 2016, pp. 21–22.
[8] Beck 2018, p. 55.
[9] Timestamping and proof-of-stake concepts more specifically explained in Nakamoto 2008, p. 2–3 and Quiniou 2019, pp. 13–14. Another consensus mechanism is called *proof-of-work* which has existed already before Bitcoin.
[10] Swan 2015, p. 37.
[11] Orcutt 2019.
[12] Beck 2018, p. 55.
[13] Beck 2018, p. 57.

Blockchain introduces a set of key characteristics which originates from the blockchain technology's dependency on a peer-to-peer network, key cryptography, and consensus mechanism.[14] The key innovation is the *removal of intermediaries* in transactions which makes the system decentralized. Blockchain enables decentralization and disintermediation of all kinds of transactions between the parties globally with an access to the Internet.[15] The techno-positive hypothesis suggests that blockchain creates a new ground for banking without banks, title transfers without central authorities, registrations without government officials, or in other words, central authority replaced with a peer-to-peer trust-based network.[16] Additionally, it is stated that blockchain technology can challenge the role of intermediaries and their role in validating transactions.[17]

Traditional transaction models, *centralized ledgers*, are based on the central authority having the role of confirming transactions, mediating, and performing other roles. In case the central authority is compromised, such as hacked or manipulated, the intruder may cause significant havoc on the system. The techno-positivists view the decentralized blockchain model, *distributed ledger*, as a better solution or an alternative for traditional transaction models: it removes the central authority and replaces it by distributing copies of the records to all parties in the blockchain. New blocks must be validated by the parties in the chain before the block is added to everybody's chain.[18] However, this does not truly state that blockchain could not be hacked or manipulated, or consider the possible downsides that the absence of an intermediary party may cause if there is no bank guaranteeing the transaction and the money is lost, for example.

In the blockchain system, being an open-access file duplicated in the network, no one is able to control the list of transactions. Every block is hashed first and then attached to the chain, which makes it unchangeable and makes the database serve as a final record of previous transactions.[19] As explained earlier, the alteration of the blockchain requires changing all the blocks in the chain, which is theoretically possible but practically quite challenging. Hashing all the blocks and timestamping of every transaction and distributed database created by the nodes verifying

[14] De Filippi 2018, pp. 33–34.
[15] Swan 2015, preface x.
[16] Mougayar – Buterin 2016, p. 118.
[17] Mougayar – Buterin 2016, p. 89.
[18] Sultan – Ruhi – Lakhani 2018, p. 52.
[19] Sultan – Ruhi – Lakhani 2018, p. 52.

the transactions creates the *trustless system*[20] that itself establishes the trust. Externalization or replacement of trust with blockchain means creating a transaction on the blockchain by *transferring the trust*[21] from a trusted intermediary to the underlying blockchain system where the trust is placed in the system. Blockchain presumes the nodes to act independently and not trusting each other, and each node requiring proof of the transaction occurred: whatever appears from the decentralized proof requiring system can be trusted to be true.[22]

Simplified, the trust is externalized from the banks or other agents and transferred into a blockchain that plays the role of the bank: to assist the transfer, to ensure the sender identity, and to assure the existence of the assets.[23] *Miners* validate new transactions and record them on the blockchain, whereas *mining* is the mechanism letting blockchain to be a decentralized system. It secures blockchain and facilitates a system without a centralized authority.[24] Blockchain is trusted by *consensus* since all the participants have similar copies of blockchain, and each participant is responsible for verifying them. This institutes a trust model based on group consensus in which the computer network, nodes, verifies the transactions and authorizes to add those into the chain.[25] *Consensus algorithm* ensures that the computer network can co-operate independently without the need to trust each other and it can continue to operate even if some participants in the network fail.[26] It is claimed that blockchain is as persistent as its community of participants decides, meaning that trusting that persistency is actually trusting the community to make the right choice.[27] It can be illustrated that the blockchain system transforms our traditional understanding of trust, which then disrupts the traditional manners of making transactions. Nevertheless, there exists different comprehension whether the system is truly trustless or is trust just transferred to a different actor.

[20] Kasireddy, 2018 argues that blockchains do not eliminate trust but *minimize the amount of trust* demanded from any single party in the system. Trust is distributed between the parties in the system that encourages the parties to co-operate with the rules defined by the system. That way the blockchain is not a truly trustless transactional system.
[21] Mougayar – Buterin 2016, p. 40 emphasize that blockchain does not eliminate trust, but sifts it. Trust is always needed, but blockchain changes how trust is given and how it is earned.
[22] Bratspies 2018, p. 19.
[23] Bratspies 2018, p. 19.
[24] Cosset 2018.
[25] Sultan – Ruhi – Lakhani 2018, p. 52. More on consensus algorithms, see also Zhang – Xue – Liu 2019, p 19–25.
[26] Rijmenam – Ryan 2019, p. 16.
[27] Bratspies 2018, p. 37. See also Mougayar – Buterin 2016, pp. 38–40.

The first blockchain system, Bitcoin, is a public blockchain in which every participant has the possibility to see all transactions.[28] However, the fear of exposing confidential data led to the development of private blockchains, which are controlled by user privileges.[29]

Public blockchain is open to read for everyone, and all participants are able to send and receive transactions.[30] Public blockchain has no single owner. The consensus process is open to all participants, and it is fully decentralized.[31] It needs the entire computer network, nodes, to agree on all changes and does not require to trust anybody participating in the network. The verification of a transaction can be done without a trusted third party, which makes public blockchain very transparent. Since the decentralization, public blockchain is harder to hack and less vulnerable to data manipulation. However, as a public blockchain is literally public to all participants it may cause privacy issues, for example.[32]

Private or permissioned blockchain is a controlled system, and only the participants can act in the chain. It is commonly used by corporations due to the limited user base.[33] Since the very few authorized participants, it has a higher transaction processing rate and requires a shorter period of time to reach the network consensus. However, as private blockchain has fewer nodes, it is more vulnerable to data manipulation and hackers.[34]

1.3 Research questions and limitations

Blockchain technology still represents a quite novel innovation even if it was first represented by Satoshi Nakamoto already over ten years ago. The regulatory problem it has caused is global, and the constant technological development is not making it easier for regulation to follow the development. The traditional territory-based understanding of state jurisdiction is not sufficient enough in itself for examining jurisdictional issues that the decentralized nature of blockchain is posing to the legislative field: in addition to the spread to several jurisdictions simultaneously, blockchain has developed a community around the technology which have certain incentive mechanisms to guide the behavior of the participants. This phenomenon has brought another perspective in the research besides the analysis on state jurisdiction: whether these new private

[28] Nakamoto 2008, p. 2.
[29] Brody 2019.
[30] Zhang – Xue – Liu 2019, p. 11.
[31] Sultan – Ruhi – Lakhani 2018, p. 53.
[32] Yang 2020, p. 2.
[33] Sultan – Ruhi – Lakhani 2018, p. 53.
[34] Yang 2020, p. 2.

subordinates, code-based communities, or specific technologies, to states have jurisdiction and how the law-like effects by private entities should be approached and governed?

The approach of this research is within the field of international law. The state jurisdiction is examined under the principles of public international law, and the perspective is horizontal, which leaves the specific contents of existing national blockchain regulation and possible conflicts between them outside of analysis by which is meant that the analysis is not comparative between national regulations, but harmonization on a more general level is considered. The legislative issues blockchain technology is posing are diverse, but the purpose is not to focus on any industry or application-specific issues. The focus is within the scope of regulatory governance of public international law and how private law, or specifically *de facto* regulation by private parties, is changing the traditional understanding of public international law and governance. Jurisdiction is a central concept as a foundation of regulatory legitimation, and regulation requires public governance. However, self-regulation is recognized as a valid concept and discussed. The traditional understandings of jurisdiction, regulation, and governance are re-examined taking into account the effects of parallel regulation development developed by a private entity, a blockchain community.

Traditionally regulation has been developed within and through the actions of public governance, whose legitimacy lies with the democratic constitution. However, public legitimacy may not form the sole ground for legislative power any longer, but private entities are able to establish rules with similar effects as law to guide behavior. Possibly the best-known form of such private power is based on the economic power of multinational corporations, but a similar phenomenon has been developing around certain technology that is based on the social power of the community, for example. The research discusses private governance and regulation from the public perspective and searches how these two could be combined into some form of hybrid governance. The two ends, private and public, are not seen as options to each other but rather viewed as a combination.

The topic of international regulation is large-scale with different dimensions – the purpose is to discuss the public regulation with private notions comprehensively but concentrate on the most relevant perspective at the time. The current state of public international regulation in relation to blockchain is analyzed with the help of two existing regulatory frameworks, but it must be noted that there are additionally developing other international regulations as well. Issues in

relation to cybercrime and criminal law are not part of this research since the criminal perspective could be a topic for another research, and it takes the analysis on the sidetrack.

The topic of this research is international blockchain regulation and regulatory governance. Therefore, the research questions are as follows: (1) How does technological determinism feature in international blockchain regulation? (2) What kind of international jurisdictional challenges exist with blockchain regulation? (3) What kind of international regulatory governance is proper for blockchain technology?

1.4 Methodology and premises

The theoretical background is based on the theory of *critical technological determinism*. Technological determinism argues that technical innovations are the primary factor changing society and culture.[35] The deterministic theories can be situated along a continuum: *harder* determinists emphasize the autonomy and power of technology while *softer* determinists allow more discretion on social control and context.[36] The functioning of blockchain is based on such technological innovations that have allowed new ways of interacting in society that were not possible before. Additionally, these acts, transactions, and commitments can occur outside the sphere of central authorities as already introduced previously. However, this research's viewpoint is critical towards the cyberlibertarian idea that technology could form a separate autonomous legal system existing in parallel with the system in the concrete world or that blockchain could not be regulated with existing tools of international law. Yet, this does not mean the denial of *de facto* effects of such a private system poses to public legislation and regulatory governance.

This research is *a legal dogmatic* analysis with *de lege ferenda* approach. The purpose of the legal dogmatic analysis is to research the current legal standing of the international blockchain regulation. After this, the analysis will focus on *de lege ferenda* viewpoint and search possible solutions for the future regulatory governance and search the proper balance between law and technology, but also public and private governance.

The relationship between technology and law is researched by using *critical discourse analysis* to identify the underlying social movement behind blockchain technology. The purpose is to

[35] Karvonen 1999, p. 82.
[36] Dafoe 2015, p. 1052.

analyze the appearance of technological determinism in the theoretical framework of international blockchain regulation, which consists mostly of the first chapter discussing the jurisdictional dimensions in relation to technology. Technological determinism in its harder expression shakes the constitutional foundation and its legitimacy as a regulator in society. This could pose a regulatory and political threat to the social order by removing the legislative power from the public authorities to technologists by creating a separate and autonomous self-regulating system.

The main references consist of articles from legal journals and publications of international organizations. Additionally, due to the novelty and technological nature of the topic, some Internet sources are found relevant. The context is based on public international law, which makes the general principles of international law and the discussion around their application to cyberspace central sources. The purpose is to link the topic of cyberspace into the real world and avoid solely abstract discussion of the nature of cyberspace. This will be done by understanding and acknowledging that private parties can affect public governance and by searching the solutions how to combine the divergent interests into a form of hybrid governance.

The structure of this thesis begins with the introduction to underlying jurisdictional premises of regulatory authority. The focus moves forward to the current standing of international regulation that is developed or could be adapted to blockchain, depending on whether a new framework is developed or an existing one is applied. The last main chapter focuses more on the *de lege ferenda* approach and seeks possible future governance developments for blockchain regulation.

2 INTERNATIONAL JURISDICTIONAL FRAMEWORK TOWARDS BLOCKCHAIN REGULATION

2.1 Jurisdictional Premises

2.1.1 Understanding of State Jurisdiction

The term *jurisdiction* refers to a general legal competence of the states, which can be divided into legislative jurisdiction and enforcement jurisdiction. *Legislative jurisdiction* refers to the power to make decisions and rules, and *enforcement jurisdiction* is the power to take action to enforce rules through the exercise of executive and judicial power.[37] The starting point is that jurisdiction is *territorial*. This secures that the national law of the state applies to all within that state. Most states claim jurisdiction over persons and events, where any part of a certain matter takes place within its territory.[38] The guiding principle is that a state cannot take actions on the territory of another state by enforcing its national laws without the consent of the latter. For example, in economic regulation, an extended form of the objective principle of territorial jurisdiction has been executed: *the principle of effective connection* may be applied as a basis for the jurisdiction where activity outside a state jurisdiction has an effect inside the jurisdiction.[39]

Due to the *decentralized nature* of blockchain, it may fall under the competence of several jurisdictions which may have different regulations:

> *"As the nodes of a decentralized ledger can span multiple locations around the world, it is often difficult to establish which jurisdictions' laws and regulations apply to a given application. There is a risk that transactions performed by an organization could fall under every jurisdiction in which a node in the blockchain network is situated, resulting in an overwhelming number of laws and regulations that might apply to transactions in a blockchain based system."* [40]

In the literature, a harmonized approach among the states has been recognized in order to receive the full potential of the technology globally.[41] The development of government

[37] Brownlie 2008, p. 299.
[38] Dorsett – McVeigh 2012, p. 39. See also Brownlie 2008, pp. 105–106.
[39] Brownlie 2008, p. 310.
[40] Salmon – Myers 2019, p. 2.
[41] Bayón 2019, p. 77.

regulation may be one of the most significant factors and risks for the adoption of blockchain technology.[42] It can be argued that the regulation will need to be largely internationally and regionally coordinated in order to receive the progressive potential of blockchain. However, the challenging question is whether the blockchain platforms, DAOs and other parts of the new ecosystems can even be regulated through the traditional way since the distributed nature of the technology.[43] Since public blockchains are, at least in theory, open for everyone to join, the jurisdictional challenges, applicable law, and appropriate risk management to transactions are more challenging to solve than with private blockchains where the parties are known.[44]

Another challenge is how a state can regulate a technology that is designed to be decentralized through a centralized institution? Or is this even the most optimal solution for technology regulation? *The horizontal regulation* could be possible through the identifiable layers in the technical structure of blockchain technology: the platform level (blockchain), the application level (the tools running on the platform such as smart contracts), and the blockchain ecosystem (such as application development and hardware). However, this would require the regulation of blockchain infrastructure, which is typically met with criticism.[45]

The challenges with the jurisdiction do not solely fall into resolving the problems with applicable law but additionally there exist *conflicts between existing national and regional regulation*. For example, due to the *immutable nature*[46] of blockchain, the data entered into the chain cannot be removed afterwards, which creates a conflict with the General Data Protection Regulation (GDPR) in the EU. According to Article 17 of GDPR, an individual has a right to be forgotten and have their personal data deleted upon request, which is hardly achievable in the decentralized blockchain network. Another issue lies with *cybercrime* and the anonymity of the participants that attracts illegal behavior. Since the self-executive nature, there are no means to retrospectively stop illegal smart contracts or other transactions from being executed.[47]

[42] Swan 2015, p. 87. See also Mougayar – Buterin 2016, p. 68.
[43] Korhonen – Ala-Ruona 2018, p. 10.
[44] Salmon – Myers 2019, p. 2.
[45] Borg – Schembri 2018, p. 190.
[46] Technically changing or removing the data is possible, but it requires changing all the blocks that follow, which is computationally hard and expensive. See Sultan – Ruhi – Lakhani 2018, p. 52.
[47] Drummer – Neumann 2020, p. 7.

2.1.2 Jurisdiction of International Organizations

The jurisdiction of international organizations in international law will be briefly discussed in this subchapter since they are subjects of law in the international plane and have an impact on society. This is relevant for the research since blockchain communities represent the powers of private actors in the international field. Theoretically, cloud blockchain communities obtain the status of an international organization due to the impact they have on society? International organizations have a role in governance which is why the role of private actors is interesting for this research. The sole discussion of the topic of creating center-oriented public governance for a decentralized system may not be relevant since private parties can be relevant actors with regard to governance as well.

International organizations can be recognized as legal persons.[48] In the *Reparation Case*[49], the International Court of Justice (ICJ) held that the organization possessed international personality and the capacity to operate on international planes. However, this does not refer to a similarity of a state, but a "super-state" meaning that it is a subject of international law and able to possess international rights and duties and able to maintain its rights by bringing international claims.[50]

Even though the Reparation Case established that international organizations are subjects of the law, it did not disclose what an international organization is.[51] According to Vienna Convention 1986 Article 2(i), an international organization means an intergovernmental organization. Further defined, an international organization refers to a collective of states established by treaty; being a subject of international law with treaty-making capacity; and has a distinct personality from its member states and common organs.[52] However, the concept of international personality does not imply the qualities of the person, meaning the international organization. There exists a difference between legal personality and legal capacity, referring to the difference between *potential ability* to exercise powers and *concrete* exercise of powers.[53] It seems that international organizations, whether having or not having legal personality, can act, and these actions should have legal consequences.

[48] Brownlie 2008, p. 648.
[49] Reparation for Injuries Suffered in the Service of the United Nations 1949.
[50] ICJ Advisory Opinion 1949, p. 179.
[51] Gautier 2000, p. 333.
[52] United Nations 1956, p. 108. See also Brownlie 2008, p. 649.
[53] Ryngaert – Dekker – Wessel – Wouters 2016, p. 16

The definition of the Vienna Convention may not represent the most corresponding definition to the 21st century, which is why other perspectives of international organizations must be considered as well. There exist many ways to classify international organizations, but *the International Panel of Social Progress* recognizes five different types of international organizations: (1) intergovernmental organizations whose members are states; (2) international non-state organizations that directly address transnational or global policy; (3) international civil society organizations; (4) international commercial organizations; and (5) hybrid public-private international organizations.[54]

It is argued that globalization and corporate political power have initiated a legitimacy crisis in democracies by hindering the role of nation state as the basis of democracy. The powers of states are increasingly discussed and negotiated with transnational private actors and put under external jurisdictions. Market liberalism has shifted into the domination of corporations and aggravated by deregulation and privatization.[55] Considering the topic of this research, private corporations and market power are not only examples of transnational private actors challenging the role of a nation state. What could be the impact of blockchain technology on a societal scale?

It can be claimed that a body exists to the extent it has *an impact* since there is a practice to measure economic or political impact, which then determines the attention given to an organization. Since many international bodies do not act to have an impact in a way that would be regarded significant to an economist or to a political scientist, they are frequently ignored in studies from such perspectives.[56] What makes the focus on multinational enterprises interesting is that they commonly, not always, represent the powers of private actors in international field. Whether or not they have legal existence under international law, they can have an impact on the society, such as an impact through affecting the behavior of individuals.

[54] International Panel on Social Progress 2018, p. 32. On the contrary, the Union of International Organizations 2021 claims that non-governmental organizations and multinational enterprises have no existence under international law.
[55] International Panel on Social Progress 2018, p. 28.
[56] Ryngaert – Dekker – Wessel – Wouters 2016, p. 16

2.2 Limitations of Territorial Jurisdiction

2.2.1 Internet Jurisdiction

Due to the omnipresent nature of the Internet and *cyberspace,* mainly the territorial models of jurisdictional competence of the state cannot be applied.[57] Even if the Internet and cyberspace may sound like synonyms to an ordinary person, there is a distinction: the Internet is a communication medium where people perform actions, but cyberspace offers ways of interacting that were not possible before, meaning that these cyberspace communities, or nets, form a difference that has matured into a difference in a reciprocal manner.[58] *Kulesza* defines the Internet as *"a global data exchange system operating based on the interconnections of local networks distributed in a number of physical locations allowing simultaneous, multidimensional worldwide interaction of users"*.[59] According to *Kuehl,* cyberspace is "*a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies*".[60] Cyberspace has three layers: a physical layer (such as computers, cables, and communications infrastructure); a software logic layer (such as algorithms), and a layer of data packets and electronics. The core of cyberspace forms a virtual space, but it is additionally supported by physical objects such as computers connecting cyberspace to the physical world.[61]

The International Internet law (IIL) is a fairly new legal field, but it has developed some core principles. The principles of law are sources[62] of international law which, however, may refer to customary law; general principles of law as in Article 38(1) of the Statute of the International Court of Justice; or to logical propositions resulting from judicial reasoning based on the existing international law. Primarily the general principles are incentive reasoning from a mass of rules, which are long and generally accepted as to be no longer directly connected with state practice.[63]

[57] Kulesza 2012, p. 30. See also Johnson – Post 1996, p. 1370.
[58] Lessig 2008, p. 83.
[59] Kulesza 2012, p. 31.
[60] Kuehl 2011, p. 28.
[61] Tsagourias 2015, p. 15.
[62] See Brownlie 2008, p. 15. Cohen 2007, p. 111 would place the international norms as the core international law and highest in the hierarchy of sources.
[63] Brownlie 2008, p. 19.

A modified principle of territorial jurisdiction adapted to cyberspace introduces modifications to traditional territorial jurisdiction according to which the effects doctrine must be adapted to the omnipresent nature of the Internet; and the jurisdiction is extended to state's country code Top Level Domain[64] which becomes cyber territory.[65] The Domain Name System (DNS) is a network of computers that connects website names with their IP addresses. Simplified, the numbers of IP address[66] allows the browser to locate the right server on the Internet and then connect to it, and in other words, DNS is a converter that converts text name into IP address.[67] The Internet Corporation for Assigned Names and Numbers (ICANN) is overseeing the DNS and is responsible for allocating new top-level domains.[68] From the techno-positive perspective, ICANN is viewed as a central authority or bureaucratic organization that is controlling the DNS and may perhaps be pressured to censor the Internet by governments and corporations. The central authority is seen as a negative institution for freedom of expression, and additionally, it can be hacked.[69] Blockchain applications, such as Handshake, state to offer a decentralized naming system where the peers in the network are validating and in charge of managing the DNS naming.[70] However, does this mean that blockchain could not get hacked or manipulated? Blockchain applications, such as Handshake, promote the idea of technological determinism and compromise the status of an authority. From a practical perspective, trusting an application such as Handshake would mean trusting a network of anonymous participants instead of central authority. Is trusting on anonymity essentially a better option since it means that there is no one responsible if some party steals domain names or conducts other criminal behavior?

The objective of the conflict of law jurisprudence is to avoid forum shopping and to offer effective dispute resolution in cases with international dimensions. Networks, such as blockchain, transfer the localization of activities for a choice of law towards the transmission endpoints, such as the place of the server location. However, the attack against the substantive law of the location of users encourages forum shopping since the location of the server

[64] This means all domains identified with a country or geographical location. Country code Top Level Domains, such as .uk for the United Kingdom and .fi for Finland, could be considered as cyber territories of their corresponding states, see Uerpmann-Wittzack 2010, p. 1256. More on domain name space regulation see Murray 2003, p. 198.
[65] Uerpmann-Wittzack 2010, p. 1254.
[66] IP means Internet Protocol and is a unique address that identifies a device on the Internet.
[67] Orcutt 2021.
[68] Roush 2012.
[69] Orcutt 2019.
[70] Handshake 2021.

infrastructure is possible to transfer into legal safe-havens.[71] For example, in the case *Yahoo!, INC. vs LICRA,* Yahoo! argued that France did not have personal jurisdiction over U.S based company that is operating via Internet from the United States and French law was not applicable, since the material was stored on the server located in the United States. The French court rejected these defenses and ruled against Yahoo! after which the company tried to go forum shopping in the United States for better outcome based on US law, but the court of appeal in the United States eventually held that the American court did not have jurisdiction over the French parties and that France had right to hold Yahoo! accountable in France.[72]

The Internet is relying on the *end-to-end (e2e)* principle, which is a classic design principle in computer networking originally adopted for technical reasons. In e2e design, the application features are located in the communication ends of the network (nodes) rather than in intermediary nodes (such as routers and gateways) that exist to establish the network. The infrastructure is operating only for transmitting information from one point to another, and the processing is happening at the endpoint. The transmission practices of the Internet are designed to be geographically independent, but the technologies and users are located within physical states, and these physical endpoints provide jurisdiction for a state to justify its authority.[73] The power systems are commonly center-oriented, where the ones in the center have power and those at the end do not. The end-to-end seems to look for the reversal of center-oriented power and a refusal of regulation and hierarchy.[74]

In the case *AT&T vs City of Portland,* the court compared the telecom arrangement to the Internet:

> *"The Internet's protocols themselves manifest a related principle called "end-to-end": control lies at the ends of the network where the users are, leaving a simple network that is neutral with respect to the data it transmits, like any common carrier. On this rule of the Internet, the codes of the legislator and the programmer agree."* [75]

With this description, the court lined that the Internet has a specific shape that should be regulated in a way that is fit for that shape, but however, this proposition does not represent a

[71] Reidenberg 2005, p. 1957.
[72] Yahoo! INC. vs LICRA 2000.
[73] Reidenberg 2005, p. 1961.
[74] Gillespie 2006, p. 446.
[75] AT&T vs City of Portland 2000.

quite neutral viewpoint. End-to-end and other characterizations for technology are somewhat polished and symbolic presentations of the shape of the phenomenon in question.[76]

As already noted before, technological development is constant, and the Internet has taken a step forward in its evolution to *Cloud Computing,* the innovation of the early 21st century. Cloud computing technology refers to *the delivery of information technology resources as a service to multiple customers through the Internet: a process whereby software, share resources and information are held on remote servers designed and established by respective network or infrastructure operator.*[77] The cloud is territorially anchored: it includes service providers and users having nationality and a domicile somewhere, and additionally, the cloud itself forms a data center that is located in constructions on the ground.[78]

Kevin Werbach introduces the *layered model* for approaching the Internet architecture and fit regulation: the replacement of horizontal approaches with vertical layers as the foundation for communications regulation. The regulation of Internet-related services is ambiguous since the horizontal categorization model under which the application of rules is based on the geographic status.[79] Additionally, the Internet jurisdiction can be approached through the *origin approach* according to which the regulatory competence should be allocated based on the origin rather than the destination of online activity.[80]

The Internet's "attack" on the state jurisdiction endorses *the technological determinism* that is highly problematic for the relationship between technology and law. This encourages the denial of state jurisdiction and transfers the rulemaking power to technologies and technologists. However, sovereign states have an obligation to ensure that technologies follow the rules of law, meaning that the states must be supreme over technological claims, but at the same time, the supremacy of law must promote innovation and the development of technologies.[81] However, the national level governance is not the only option, even if coordinated at the supranational level. The international governance will be discussed more comprehensively later in this research.

[76] Gillespie 2006, p. 429.
[77] Cheung – Weber 2015, p. 8.
[78] Cheung – Weber 2015, p. 121.
[79] Werbach 2002, p. 18.
[80] Tsagourias – Buchan 2015, p. 49.
[81] Reidenberg 2005, p. 1969.

2.2.2 Cyberspace Jurisdiction

Cyberspace can be defined as a set of individual and interconnected electronic communications networks. The Internet itself is not a physical object, but it has evolved as a multitude of network protocols adopted by individual networks allowing the transfer of information between them. The connection between the Internet and cyberspace is that the Internet takes the user to a separate place, cyberspace, and additionally, nobody is able to exist in cyberspace without an Internet account. Cyberspace is not a physical location but an electronic place that is different from the physical characteristics of the real world where electronic transactions and life can exist, affecting the physical life.[82] The separateness of cyberspace is explained through its interdependence of the physical world: interactions in cyberspace are independent of space constraints and conducted without physical acts. Nevertheless, it can still be said that cyberspace consists of a physical layer as well since computers and other communications infrastructure are physical objects in a physical world.[83]

It is argued that cyberspace could be treated as *a separate place* where a distinct regulation applies, and cyberspace would have distinct laws applicable to cyberspace. It would be much easier to be certain which rules apply to cyberspace transactions than to determine which territorial-based state may apply its laws to these transactions.[84] Could cyberspace develop its own legal system? According to *Johnson & Post,* the cyberspace could *self-regulate* itself since there is a need for a separate legal system defining the interactions in cyberspace since it cannot be subject to sovereignty due to its a-territorial nature. This is because the cyberspace activities occur in several jurisdictions at the same time, and the persons or entities transacting cannot know if the activity causes effects in a particular jurisdiction, and additionally causing issues in relation to governing law.[85] On the contrary, *Goldsmith* argues that sovereigns are able to regulate the local effects of extraterritorial activities. According to him, the potential of traditional legal tools and technology are underestimated in resolving the multi-jurisdictional challenges implicated by cyberspace, and cyberspace transactions are not less resistant to the conflict of laws tools than other transnational transactions.[86] Additionally, *Tsagourias* supports

[82] Zekos 2007, p. 2.
[83] Tsagourias 2015, p. 15.
[84] Johnson – Post 1996, p. 1380. See also Barlow 1996.
[85] Johnson – Post 1996, p. 1367. See also Lessig 2008, p. 2.
[86] Goldsmith 1998, p. 1200.

the viewpoint that traditional legal tools can solve the multi-jurisdictional issues connected to cyberspace and, in this manner, overcome issues of legitimacy.[87]

In theory, it could make sense that cyberspace would form a separate regulative system, but can the cyber community declare the sovereignty of cyberspace? The cyberspace community does not constitute "*a people for self-determination purposes*"[88] since the membership of the cyber community is infinite: the users may be conscious of being cyberspace users, but the users are placed in their own states who live in concrete spaces. Additionally, they live in geographic spaces and are under the jurisdiction of their respective states. Cyberspace lacks institutional, normative, and legal structures to support sovereignty. Therefore, cyberspace does not have its own "people", independence, and mechanisms to claim internal and external sovereignty.[89] There is a confusing difference when conceptualizing cyberspace: cyberspace can be understood as a separate place, but this should not be mixed with the ideology that cyberspace should be regulated as an independent regime.[90]

Menthe would recognize cyberspace as the fourth *international common,* in addition to Antarctica, outer space, and the high seas, based on the theory of international spaces and the status of Common Heritage of Mankind (CHMK)[91] given to elements constituting a particular space.[92] The *res communis*[93] is not subject to the sovereignty of any state, and states are obliged to refrain from all acts which may harmfully affect the use of the space by other states or their nationals.[94] The jurisdiction of international commons is commonly based on *nationality* instead of territory, such as in the Law of the Sea Convention of 1982, Article 92(1) states that Ships shall sail under the flag of one State only, and save in exceptional cases expressly provided for in international treaties or in this Convention, shall be subject to its exclusive jurisdiction on the high seas. However, the application of "the law of the flag" principle from

[87] Tsagourias 2015, p. 17.
[88] This refers to the legal right of people to decide their own destiny in the international order (the principle of self-determination). The right of cohesive national groups to choose for themselves a form of political organization and their relation to other groups. See Article 1 of the Charter of the United Nations, see also Brownlie 2008, p. 580.
[89] Tsagourias 2015, pp. 23–24.
[90] Hunter 2003, p. 443.
[91] See United Nations Convention on the Law of the Sea, Article 137(1).
[92] Menthe 1998, p. 70.
[93] means a "common thing", that certain areas and resources are vested in the international community as a whole and are not subject to specific purposes by any state. The principle was originally adopted to concern the high seas but is now generally recognized to cover additionally outer space and other supranational bodies having the same general characteristics. See Grant – Barker – Parry 2009, p. 520.
[94] Brownlie 2008, p. 169.

international maritime law to cyberspace is not that straightforward. In cyberspace, nationality is brought to the international space of cyberspace by the persons via their actions. According to *Menthe*, the nationality of items in cyberspace could be defined based on the nationality of the person or entity, who places the items into cyberspace, or possibly by the party who controls them.[95]

In cyberspace, web pages could function as a determinant for nationality, which means that the person or other entity creating the link to a certain webpage would be subject to the legal system regulating the references made by that party. The authors may be held as the responsible party for electronic content in accordance with the laws of their nationality. The same jurisdictional analysis would be applicable to the links to other web pages in cyberspace.[96] Another approach to cyberspace jurisdiction is to treat the server as the physical location for the purposes of asserting territorial jurisdiction.[97] However, this might be too complex since the vast number of servers.

In addition to the Internet jurisdiction, cyberspace jurisdiction presents points of view that support technological determinism, such as regulating cyberspace as an independent legal regime. Cyberspace is connected to the physical world through the physical layer, and the existing multijurisdictional tools are able to solve jurisdictional challenges. Cyberspace jurisdiction seems to present a somewhat similar ideology as internet jurisdiction by denying state jurisdiction, which supports the cyberlibertarian viewpoint.

2.3 Jurisdiction of New Private Subordinates

Blockchain technology challenges the traditional role of the state by allowing individuals and communities to interact in society in unprecedented ways. Technology enthusiasts even present that the society could be able to organize itself more effectively via blockchain technology-based services instead of traditional functions of states.[98] The rapid technological development may cause unclear rules and areas of legal ambiguity since the governments and public regulators frequently come after the development. The consequence of the inability to follow technological development is that the private actors begin to develop their own standards.[99]

[95] Menthe 1998, p. 93.
[96] Kulesza 2012, p. 146.
[97] Menthe 1998, p. 79.
[98] Atzori 2017, p. 46.
[99] Fosch Villaronga – Golia 2019, p. 130.

Catá Backer describes *global law* as the law of non-state governance systems. It is a management system of universe autonomous governance frameworks that is based on the functional differentiation of governance communities and global operation.[100] Globalization has an impact on the role of the state and the understanding of state-oriented legislation. In relation to globalization, the law needs reconstruction since it is put under an attack of parallel informal systems of legal ordering.[101] However, the governance communities governed by global law are not necessarily organized similarly as states, such as geographic territory, but can be seen as societies organized for mutual benefit for certain objectives.[102]

It is implied that blockchain is creating a process of *institutional entrepreneurial discovery*: entrepreneurial activity is creating market-based solutions to issues that are commonly taken care of by the government. Blockchain technology enables transparent and immutable recording of socioeconomic facts whose rules can only be changed by uniform consensus, which is lowering the costs of voluntary organizations at the expense of public governance structures.[103] The existence of these non-governmental organizations no longer depends on state recognition, but these entities obtain autonomy and governance power. These entities, centrally multinational corporations, have the power similar to the state, and they are able to exercise governance authority within their own value chains that is reminiscent of the legislative authority of states. However, the authority can additionally absorb other forms, such as standard setting, certification organs, or share practices, such as cyber-communities.[104]

The autonomy held by transnational corporations is not similar or comparable to binding legislation laid down by national parliaments, but it has rather changed the relations between the state presented public law and the private actors within the nation state. Nevertheless, the rising autonomy of private actors is shaking the traditional hierarchical structure where state rules are regarded as hard law and the rules of transnational corporations as soft law.[105]

> *"In this network the government has a place, but not a primary or controlling role. In many cases it is noticeable by its absence. Contract replaces law; networks of relationships replace a political community; interest replaces territory; the regulated becomes the regulator."* [106]

[100] Catá Backer 2012, p. 177.
[101] Zumbansen 2013, p. 121.
[102] Catá Backer 2012, p. 181.
[103] Berg – Markey-Towler – Novak 2020, p. 3.
[104] Catá Backer 2012, p. 183.
[105] Gunther 2012, p. 47.
[106] Catá Backer 2008, p. 26.

The more central role of the global entities appears to be somewhat unquestionable, but whether the "either-or" viewpoint is a proper setting for analysis is another question. In relation to blockchain, the technology enthusiasts have strong beliefs in the potential of the technology and its ability to override the public regulators. Instead of an "either-or" discussion, the more beneficial one would be "both public regulators and private entities" and the establishment of governance where both sides can co-exist.

2.4 Jurisdiction of Autonomous Code-based Communities

2.4.1 Lex Informatica

The analogy towards a separate law of cyberspace originates from *Lex Mercatoria*[107] [108] which was a new legal system originally developed in the Middle Ages for the purposes of cross-boundary trade. The same kind of phenomenon has been developing in the cyberspace.[109] The general implication that Lex Mercatoria has is the claim that it constitutes an autonomous legal system, and therefore there can exist privately constituted legal systems that are independent of the state.[110]

The ideology of a separate cyberspace legal system was introduced by *Reidenberg* due to the complexity to regulate the phenomenon on a national level:

> *"In the era of network and communications technologies, participants traveling on information infrastructures confront an unstable and uncertain environment of multiple governing laws, changing national rules, and conflicting regulations."* [111]

It is argued that cyberspace cannot be treated through multiple jurisdictions, but it should rather be treated as separate jurisdiction where its own rules and laws reflect its special nature.[112] The treatment of digital information should be more predictable and stable, and the current

[107] Lex Mercatoria was created in the absence of "world legislator" where international trade developed functional rules based on a common practice. More comprehensively, see Windbichler 2015, p. 916.
[108] A similar process can also be discovered in *lex laboris internationalis* (international labour law) where "enterprises and labour unions as private actors are dominant law-makers". See Teubner 1997, p. 157.
[109] Johnson – Post 1996, p. 1390.
[110] Zumbansen 2013, p. 123. On the contrary, Teubner 1997, p. 156 argues that Lex Mercatoria is not law since it is not based on a hierarchy of legal rules but is rather social rule or custom. However, even if Lex Mercatoria would not be seen as law, it is *a positive law*.
[111] Reidenberg 1998, p. 554.
[112] Mefford 1997, p. 222.

conflicting policies between the nations show a lack of harmonization.[113] The transnational nature of cyberspace and the conflict of several jurisdictions created the ideology of *Lex Informatica* – the law of the Internet.

Already in 1996, *John Perry Barlow* declared the independence of cyberspace, the world that is everywhere but in which nobody lives.[114] Additionally, *Johnson & Post* offered a solution to treat cyberspace as a distinct place from a physical world for legal analysis.[115] According to *Mefford*, Lex Informatica could meet the ends of legitimacy, power, and effectiveness by justifying and explaining legal authority that has not been met by jurisdictional law.[116]

Lex Informatica would trust the flexibility of private actors to create commonly agreed standards and reflect the generally accepted principles such as equity and stability.[117] Lex Informatica is a set of rules independently developed by the international Internet community which is offering an alternative system based on self-regulation consisting of customary law and technical norms that is operating on international level sovereignly of domestic laws and allowing the interoperability of the Internet.[118]

Lex Informatica has the central elements of the legal system (Table 1). In theory, Lex Informatica could form a parallel legal system. The jurisdiction of Lex Informatica is not based on territorial borders but on a network and its locations where the source of law[119] is technology developers and customary rules instead of state authority.[120]

[113] Reidenberg 1998, p. 554.
[114] Barlow 1996.
[115] Johnson – Post 1996, p. 1378.
[116] Mefford 1997, p. 235.
[117] Fishman 1999, p. 91.
[118] Fyrigou-Koulouri 2018, p. 9.
[119] More on the sources doctrine, see Brownlie 2003, pp. 3–4.
[120] Reidenberg 1998, p. 570–571.

Table 1. Lex Informatica.

	Legal Regulation	Lex Informatica
Framework	Law	Architecture standards
Jurisdiction	Physical Territory	Network
Content	Statutory/Court Expression	Technical Capabilities Customary Practice
Source	State	Technologists
Customized Rules	Contract	Configuration
Customization Process	Low Cost Moderate cost standard form High cost negotiation	Off-the-shelf configuration Installable configuration User choice
Primary Enforcement	Court	Automated, Self-execution

Lex informatica is depending on the development of rules based on network, technical standards, and protocols to regulate *the flow of information.*[121] For a legal system to be effective, it must be seen as legitimate, meaning that it needs the consent of the governed. Otherwise there exists a risk of ignorance of the law and increased enforcement costs.[122] However, the concept of Lex Informatica has received skepticism about whether the technical standards are capable of defining the limit of cyberspace and acceptable behavior.[123] Lex Informatica represents the ideology of technological determinism by transforming the legislative power from the state to private parties of blockchain. The purpose is not to undermine the power of technology to change the society since it has happened before with the World Wide Web, for example, but instead of either–or positioning between the private and public a coexistence and co-operation could result in more stable outcomes. It seems that Lex Informatica supports perhaps the harder technological determinism since the complete legal regulation is transferred to technology, and other social factors are not recognized.

[121] Fishman 1999, p. 101.
[122] Mefford 1997, p. 217.
[123] Goldsmith 1998, p. 1213. See also Fishman 1999, supra note 6.

2.4.2 Lex Cryptographia

The rise of the Internet led to the formation of Lex Informatica, but the development of blockchain technology might develop another set of rules called *Lex Cryptographica,* which is managed through self-executing smart contracts, decentralized (autonomous) organizations, and algorithmic governance.[124] *Goldsmith & Wu* argues that the rise of networks, groups of computers connected for communication, did not actually remove the intermediaries but rather changed who they are. It created a large number of new intermediaries of which the most important are Internet Service Providers (IPS), physical network, browsers, search engines, and financial intermediaries. The Internet has created the network itself as an intermediary for much communication and conduct that had no intermediary prior Internet.[125] *Wright and De Filippi* propose that the use of decentralized technology can be controlled by regulation via (1) threat of law enforcement, (2) the market manipulation, (3) developing new social norms, or (4) putting pressure on intermediaries such as IPSs, social networks or search engines.[126]

Laidlaw presents the model of Internet Information Gatekeepers (IFG), who are the parties controlling the information flow, deliberation, and participation on the Internet and the democratic, which is not restricted to the concept of representative democracy. IFGs include ISPs, search engines, social networking sites, and portal providers. Gatekeepers are divided into *macro-gatekeepers*, *authority gatekeepers,* and *micro-gatekeepers* (Figure 1) depending on the extent to which the information has democratic significance and the reach of the communicative space. The level of responsibility depends on the amount of impact the gatekeeper has on the democratic culture.[127]

[124] Wright – De Filippi 2015, p. 48. Algorithmic governance and concept of governance in this context will be discussed in subchapter 4.2.1.
[125] Goldsmith – Wu 2006, p. 70.
[126] Wright – De Filippi 2015, p. 48.
[127] Laidlaw 2010, pp. 271–274.

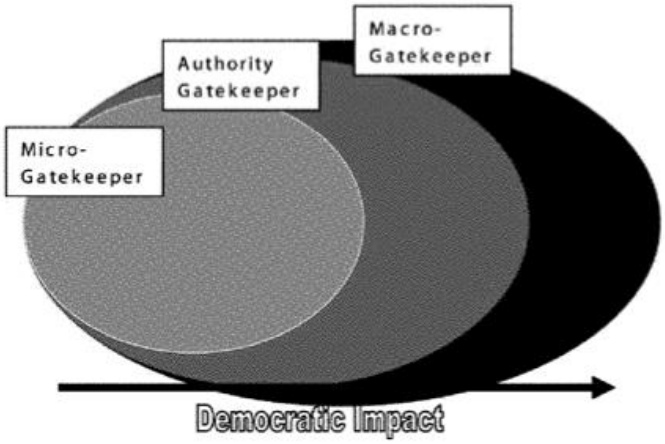

Figure 1. The Model of Internet Information Gatekeepers.

The *Pathetic Dot Theory* (Figure 2) is created by *Lawrence Lessig,* according to which there are four forces regulating the lives of individuals: the law, social norms, the market and technical infrastructure (architecture). Pathetic dots are the lives of individuals and the regulation of the dot is the sum of all four forces where any change in any one of the forces has an effect on the regulation of the whole.[128]

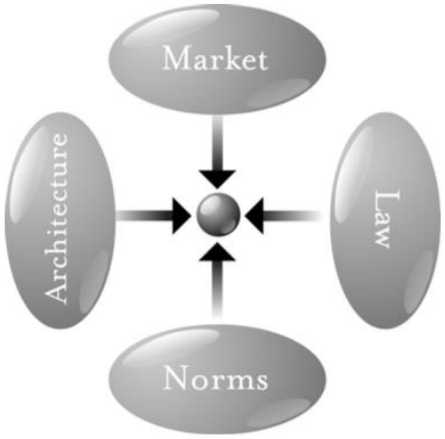

Figure 2. The four forces of regulation.

It is argued that practice has strengthened the Pathetic Dot Theory: laws are passed to ban online services; private interests (or sometimes governments) manipulate markets by pressuring search engines and advertising networks; regulators try to preserve social norms, but at the same time,

[128] Lessig 2008, p.122.

they are trying to control the information that individuals are exposed to.[129] The law enables legal sanctions by defining the behavior that can be carried out to avoid legal consequences. Commonly national legal sanctions refer to the legal punishment measures, which are for legal norm enforcement and prevention of misconduct.[130]

However, it is recognized that law is not the only regulator[131], but social norms are as well. Norms control human behavior, but unlike law, the punishments are not centralized. The enforcement of norms is executed by the community and not the government.[132] Not only can regulatory rules regulate the social activity, but the private online communities are subject to invisible consensus rules that are in practice regarded as rules since they are deeply part of their everyday lives. These rules are not only creating but additionally determining and controlling a type of behavior.[133] Technology can be used to create rules and organizational structures for entities and even governmental bodies. Smart contracts may have the ability to rewrite or bypass the core principles of contract law by turning property rights as a subset of contract law.[134]

Murray represents another approach on how to understand cyber-governance: the premise is that an individual is not isolated like the pathetic dot and under the influence of an external control system. In this model of *network communitarianism* or "active matrix theory", the pathetic dot is replaced with a networked community (matrix) of dots that are sharing ideas and opinions. Secondly, the laws and norms get their legitimacy from the community (matrix of dots), which makes the regulatory process a dialogue, not an external system (Figure 3).[135]

[129] Wright – De Filippi 2015, p. 49.
[130] Jansen 2019, p. 422.
[131] The Critical Legal Studies represent a vision according to which the law is not objective and non-political but is tied to social systems and questions. The law is not neutral but a mechanism to legitimate structures of political and economic power. See Singer 1984, p.6.
[132] Lessig 1999, p. 507. See also Lessig 2008, p. 125.
[133] Jansen 2019, p. 421.
[134] Wright – De Filippi 2015, p. 50.
[135] Murray 2011, p. 205.

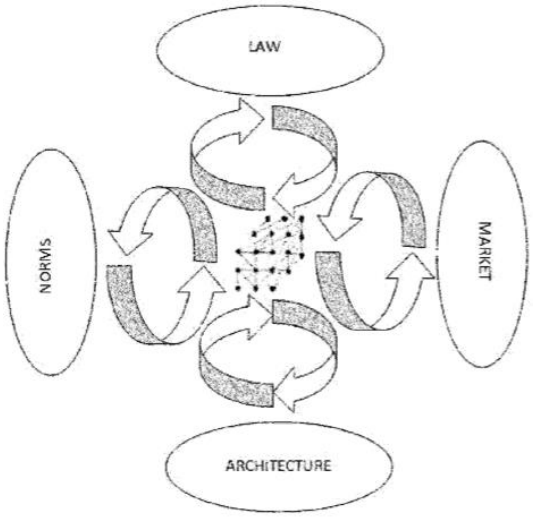

Figure 3. Network Communitarianism.

Lex Cryptographia supports the idea of cyberspace jurisdiction and the treatment of cyberspace as a separate place in which distinct laws of cyberspace would apply. Lex Cryptographia illustrates the technological determinism and creates a somewhat "cyber bubble" away from regulatory reach, which nevertheless is an incorrect assumption since cyberspace can be controlled and regulated even if it may require stepping outside the traditional understanding of territorial jurisdiction. However, compared to Lex Informatica Lex Cryptographia possibly supports a softer approach to technological determinism since it considers other determinants in society that can control human behavior and not just solely technology.

2.4.3 Code is Law

Code is law represents the idea that code can function as law and regulate cyberspace as *Lawrence Lessig* first introduced it: "*Life in cyberspace is regulated primarily through the code of cyberspace. Code is a regulator in cyberspace because it defines the terms upon which cyberspace is offered. And those who set those terms increasingly recognize the code as a means to achieving the behaviors that benefit them best*." [136] Briefly, "Code is law" forms a regulation in which technology is used to enforce existing rules. A new phenomenon is occurring around blockchain technology, where technology is increasingly taking over these rules.[137]

[136] Lessig 2006, p. 84.
[137] Hassan – De Filippi 2017, p. 88.

The "Code is law" based thinking seems to represent a form of implementation of Lex Informatica and Lex Cryptographica, and is additionally taking technological determinism to the next level, towards practice and implementation. It must be recognized that the legal code (the law) and technical code are not the same, which may be somewhat misleading to say that code could be law. Legal rules determine what people shall or shall not do, where technical rules determine what people can or cannot do.[138] Legal code, rules consisting of legal obligations are *extrinsic,* meaning that the rules can be breached, but there is a consequence from breaking the rules ensuring compliance. On the contrary, technical code is *intrinsic*: an error occurs if the rules are broken, and no activity occurs, which means that the compliance is ensured through the code itself.[139] The issue with the code is the automated execution that occurs even if the outcomes are undesired or unforeseen.

The code-based rules could have the potential to bring benefits into the society by automating the law and enforcing rules *a priori*. Blockchain system has already proved its ability to function without legal rules, and instead the followed rules are defined and enforced by the code.[140] However, the code is not neutral but, in principle, political, which has societal implications and might support certain political structures or actions and behavior.[141] Technology may have similar capabilities to influence human behavior as law. Nevertheless, opposite to law, technology relies on stiff rules and technical features and does not leave much room for coders to decide the course of action.[142]

Even if the code is not sufficient enough to function as law by itself, with the regulation there are not only two opposite possibilities: to regulate by law or let the code regulate. As it has already been seen with the Internet, which has created a global interconnection without the establishment of an international legal regime, but the development of a formal legal regulatory regime could risk the growth and innovation.[143] *Machine learning (ML)* could offer some kind of solution to the balance between the code and law. ML allows software to acquire knowledge from outside sources in order to learn and operate that was not specifically programmed into it. With ML, it would be possible to circumvent at least some of the limitations commonly related

[138] Lessig 2006, p. 82.
[139] Walport 2015, p. 41.
[140] Walport 2015, p. 42.
[141] Hassan – De Filippi 2017, p. 89.
[142] De Filippi 2018, p. 194.
[143] OECD 2011, p. 6.

to code-based regulation.[144] Still, it must be kept in mind that automated decision-making based on data may be biased and thereby unfair.[145]

The role of technology has changed since the discovery of the Internet and the evolution of digital technology. Technology is not seen as a phenomenon beside the law that influences human behavior, but the code has become a level of regulation used by private and public institutions to shape functions that often extend beyond the law.[146] Code is law supports technological determinism by suggesting that technology could take over legal rules, which is reasoned with the nature of cyberspace that is ultimately created by the code, which is why code should be the best way to regulate cyberspace. However, it can be recognized that code may not necessarily be neural but subject to politics which is why other societal implications may additionally influence human behavior. It could possibly be said that code is law may not be as hard technological determinism as it first appeared since it considers other social factors as well.

[144] Hassan – De Filippi 2017, p. 90.
[145] Hardt 2014.
[146] De Filippi 2018, p. 195.

3 THE FORMATION OF INTERNATIONAL REGULATION

3.1 Guiding principles

The starting point for online law-making is that there exists an equivalence in the offline world. According to *the principle of functional equivalence,* the same principles should regulate online activity equal to the ones that are applied to the equivalent offline activity.[147] However, online activity or electronic communication cannot be considered as a clear equivalent of paper-based documents and communication since it is different in nature and does not necessarily fulfill all functions of a paper document. For example, the requirements such as "signature", "original", and "writing" must be extended to encompass the techniques used online.[148]

The challenge with this principal principle is the broad meaning of equivalence and how the equivalence can be actually achieved. An ambiguous guideline could be the principal functions as a guideline for the application of existing law or the creation of new law. However, a more concrete solution might be that the same rule should apply to both online and offline activities.[149] The focus of analysis should be the purposes and functions of paper-based documents with an intention to determine how these purposes and functions can be transformed and fulfilled with online techniques.[150]

The principle of technological neutrality means that the given rules do not depend on or require the use of certain types of technology, and the rules can be applied to all types of information and communication. Technological neutrality is important to ensure that the law is able to accommodate technological innovation and development without becoming quickly dated.[151] *Thompson* describes that the role of technological neutrality is to ensure non-discrimination that could otherwise occur through regulation, and additionally, the role of law is not to describe the specificities of technological creations.[152]

[147] Reed 2010, p. 249.
[148] The Convention on the Use of Electronic Communications in International Contracts 2005, para. 47–48.
[149] Reed 2010, p. 250.
[150] The Convention on the Use of Electronic Communications in International Contracts 2005, para. 51.
[151] The Convention on the Use of Electronic Communications in International Contracts 2005, para. 48.
[152] Thompson 2012, p. 307.

3.2 Theoretical regulatory premises

According to one survey, regulatory uncertainty is recognized as the biggest obstacle to blockchain adoption.[153] *Mougayar & Buterin* compares the regulatory standing of blockchain to *innovator's dilemma*: regulated companies have challenges to exempt themselves from existing regulation they must comply with, and with technology, they must implement it within the approved zones of regulators.[154] On the other hand, there exist states that profile themselves as *blockchain hubs* which refers to fast-growing states based on the development of their technological, digital, and regulatory infrastructure, cryptocurrency trading volume, and patent applications, for example. These states, such as Singapore and South Korea, have leveraged the intensity of entrepreneurial activities to shape themselves into blockchain hubs which are appearing in their regulatory support for these activities.[155]

In the previously discussed *Pathetic Dot Theory,* the behavior of an individual can be controlled through laws, social norms, market forces, and architecture. Individual's behavior can be influenced through passing laws or through more subtle ways, such as creating social norms, using taxes for market regulation, and constructing architectures of the physical or digital world.[156] Even if the theory can be criticized for the requirement of perfect predictability[157], it illustrates that traditional laws are not the only ways to affect behavior competently.

The emergence of *Lex Informatica* and *Lex Cryptographia* has formulated a challenge for regulatory governance. Due to the autonomous nature of blockchains, the object of regulation (the pathetic dot) – the blockchain itself can be said to be disappearing: even if the blockchain may have been designed to ignore the law, it is depending on new intermediaries supporting the network, which are the object of regulation.[158] However, the theoretical framework represents technological determinism and sees the technology as the determining factor in user behavior which undermines *the user autonomy*; meaning that the behavior of users cannot be taken as a constant and only controlled by technology. The autonomy means that the users will continue to act in their own way in the absence of intervention, and therefore, regulation cannot

[153] Based on PwC's Global Blockchain Survey 2018, 48% of the responders considered regulatory uncertainty within the top 3 barriers to blockchain adoption. However, there exists a difference between commercial activities: it is expected that the financial sector may face more regulatory challenges than industrial products, energy and retail, for example.
[154] Mougayar – Buterin 2016, p. 80.
[155] Wang – Ren – Lim – Lo 2019, p. 1.
[156] De Filippi 2018, pp. 173–174.
[157] See Leiser 2016, p. 192.
[158] De Filippi 2018, p. 17

see the behavior of those being regulated as unchanged. Regulation will cause changes in the behavior and outcomes that are unintended.[159]

Decentered regulation offers an opposite alternative to traditional government-created "command and control" regulation. Decentered regulation is based on a changed understanding of the relationship between government and society. It illustrates the ideology that other orders besides the law can have regulating effects.[160] Decentering refers to a shift in the activity of regulating from state to other, several locations.[161] Regulation is moving towards horizontally constituted regulation in which states participate but do not necessarily subordinate.[162] However, decentered regulation is also described as informal or having obscure legal effects.[163]

Self-regulation has been identified as a possible approach to regulate blockchains and was presented earlier with cyberspace jurisdiction. However, it must be discussed how self-regulation is understood in this context. Traditionally, there is no unequivocal definition for self-regulation, but commonly it involves a group of professionals developing a code of conduct and other rules regulating standards, actions, and behavior.[164] This can be understood as an *internal regulation* of an entity, such as a multinational corporation.[165] Still, the more interesting aspect is the *external regulation*, external corporate constitution, which is seen as a self-constituting essential organizational framework inside the entity and its interaction where it autonomously regulates behavior among its stakeholders. The entity discontinues to be only as an object of law and has a self-regulatory role, but the nature of self-regulation is different since the entity reverses roles with the state and becomes a consumer of regulation.[166] Through external regulation, the entity is able to harmonize behavior among a large set of stakeholders within strict bounds of the relationships between them. This form of self-regulation through private standard-setting initially in the background has attained a more central role in recent decades, which is offering an effective institutional foundation associated with the state and its legislative authority.[167]

[159] Black 2001, p.108. See also Leiser 2016, p.193.
[160] Smith 2004, p. 444.
[161] Black 2001, p. 113.
[162] Catá Backer 2011, p. 760.
[163] Smith 2004, p. 444.
[164] OECD 2002, p. 6.
[165] Catá Backer 2011, p. 762.
[166] Catá Backer 2011, p. 763.
[167] Zumbansen 2011, p. 56

The functional approach represents the value of existing legal rules and their application to new technology in order to address legal uncertainty in a timely manner instead of implementing new legal rules that may be unworkable, unsuitable or even unnecessary.[168] The idea is to identify the central features of the developed technology in concern and to govern existing rules, and see how these could be transferred into the context of the new technological development.[169] The central assumption of the approach is that even though blockchain is a new technology, its functions are not necessarily unknown to the legal system.[170]

One approach to divide existing regulatory strategies is as follows: (1) *Wait-and-see*, (2) *Issue Narrowing or Broadening Guidance*, (3) *Sandboxing*, (4) *Issue New Legislation* and (5) *Use Blockchain Technology for Their Own Purposes*.[171] According to the wait and see strategy the existing regulation can be applied while waiting on how the technology will develop.[172] After gathering the information via observations of the technology, informal guidance on the application of existing frameworks can be issued. However, there is no question on adopting new legal rules but providing guidance to stakeholders on the interpretation.[173] A regulatory sandbox is a tool that joins regulators, corporations and technological experts to test new technological innovations and solutions in order to identify obstacles arising in their deployment.[174] The regulatory sandbox offers possibilities for regulators to test new innovations and adjust the regulatory approaches in order to predict when the political atmosphere is viable for the adoption of the regulatory approaches on a larger scale.[175] In the last strategy, legislators can rely on DLT to optimize its own process. This may not be an actual regulatory strategy but enables regulators to learn about the DLT by testing it themselves.[176]

3.3 The Emerging Role of Transnational Law

The tradition of defining law as the law of a nation state established a domestic legal system where law-making is based on national sovereignty and administered by the national court system. Affairs in relation to more than one country are covered by the public international law,

[168] Gikay 2019, p. 33.
[169] Twigg–Flesner 2016, p. 3.
[170] Gikay 2019, p. 34.
[171] Finck 2017, pp. 675–682.
[172] As an example, see a European Agenda for the Collaborative Economy, COM (2016) 356 final, p. 1–2.
[173] Finck 2017, p. 676.
[174] European Commission 2020.
[175] Allen 2019, p.646.
[176] Finck 2017, p. 681. See also Mougayar – Buterin 2016, p. 68.

meaning the relationships of different states to each other and the rights of international organizations. However, through globalization, transnational matters do not only involve solely states, but corporations and other (private) groups and entities. *Transnational law* is understood more broadly than public international law meaning that it addresses all cross-border matters emphasizing the role of private actors in a globalized world.[177]

Globalization has broken the ideology of the nation state with its public authorities as ultimate legislators. Even if there exist arguments on both sides, whether, for example, Lex Mercatoria is actually law, it represents a notion of transnational law where "private governments" practice norm-production.[178] Transnational law considers the distinction in the nature of law and non-law, which it understands as an expression of its own need to define its relation to society.[179] *Calliess* calls transnational law as *a third category of law* that is between national laws and public international law that is an autonomous legal system beyond the state. These overlapping and competing jurisdictions develop around specific issues that are functionally differentiated from global society since their emergence is issue-focused on certain subjects.[180]

Even if the birth of transnational law is recognizable, it leaves unanswered the question: what is the democratic legitimation of these "private governments" producing norms beyond a state? Despite their legitimation, they are exercising law-making *de facto* and producing *positive law* which needs to be obeyed willingly or unwillingly. This establishes the need to look for new forms of democratic legitimation of private government that would bring this action of "private law-making" under public control.[181] The formation of such private governments and legal systems raises issues in relation to the impact of these institutions that are developing alongside national and (public) international regulatory systems. Additionally, the discussion is not necessarily solely around the development of private governments but even a larger phenomenon. The global legal order is facing constitutionalizing issues in relation to accountability and legitimacy, which the developing transnational regulatory systems do not have and which are developing outside of the sphere of public international law.[182]

[177] Calliess 2002, p. 186.
[178] Teubner 1997, p. 157.
[179] Zumbansen 2013, p. 132.
[180] Calliess 2002, p. 187.
[181] Teubner 1997, p. 159.
[182] Calliess – Zumbansen 2010, pp. 33–34.

Blockchain in nature is more than just a technological development, but a social technology that can be used for coordinating individuals. *Lex Cryptographia* operates without state authority, and the absence of hierarchy and enforcement structures are the aspects of the crypto environment. Blockchain network functions under a form of an economic theory of value rather than legal theory where crypto economics encourages blockchain network to act in ways that reduce the likelihood of harmful behavior for the individual and social welfare of the crypto society.[183] Blockchain society has developed a framework similar to Lex Mercatoria. There exists standing ground for legal debate whether blockchain is an autonomous legal system beyond a state, which viewpoint is highly supported by the technology enthusiasts and represents the viewpoint of technological determinism. However, possibly the more important question here is, instead of blockchain as a legal system, how blockchain can and should be governed since it has the ability to create notions similar to positive law through affecting the behavior of the individuals?

3.4 Regulatory Frameworks – Developing A New Framework or Adapting Existing Regulation?

3.4.1 International Telecommunication Union

The International Telecommunication Union (ITU) is functioning under the United Nations (UN) and is specialized in information and telecommunication technologies. The main focus of ITU is the recommendations and standards defining the operation of telecommunication networks.[184] ITU issued a *Distributed Ledger Technology (DLT) Regulatory Framework* in 2019 focusing on the topics concerning DLT regulation, including the properties and risks of DLT, regulatory challenges and recommendations for regulators and users.

The regulatory challenges are divided into categories based on the DLT features as follows:

- Property 1: Distribution, shared ledger
- Property 2: Autonomy and responsibility
- Property 3: Tamper evidence and resistance
- Property 4: Incentive mechanism and digital assets
- Property 5: Openness and transparency/anonymity

[183] Dimitropoulos 2020, p. 1152.
[184] ITU 2020b.

The corresponding regulatory challenges are recognized by ITU in Table 2. In the following paragraphs, these features with corresponding regulatory issues will be discussed, including the proposed regulatory recommendations by ITU.

Table 2. DLT Features and regulatory challenges.

Feature	Examples of regulatory challenges
Distribution, shared ledger (no central repository) [b-Yaga]	1) Applicable law with respect to nodes established in different states; 2) Legal subjects in multiple jurisdictions; 3) Distributed storage solutions to meet the requirements of production environments; 4) Interoperability requirements; 5) New civil or commercial-law forms, organizations and contracting; 6) Protection of secrecy in open environments.
Autonomy and responsibility	1) Legal smart contract definition and enforceability (valid source code execution); 2) Boundaries of anonymity; 3) Applicable law; 4) Liability of smart contract managers (SC layer governance); 5) Intellectual property of code.
Tamper evidence and resistance	Regulation that requires the correction or removal of data in the ledger, for example: 1) data protection laws / right to be forgotten; 2) content that infringes on third parties' rights (e.g. copyright, trademark etc.); 3) illegal content.
Incentive mechanism and digital assets [b-FINRA, b-Yaga]	1) Coin, token, tokenization legal common (UNCITRAL) definition; 2) ICO definition and minimal requirements for investor protection; 3) Crypto asset/token financial system: legal concept and boundaries; 4) Supervisory policies and procedures in accordance with applicable rules [b-FINRA].
Openness and transparency/ anonymity	1) AML issues, secrecy leaks, personal security [b-FINRA]; 2) Anonymization (no name/encrypted users vs KYC) and pseudonymization [b-EU-a].

The DLT is based on *sharing data* among several systems that are set in different locations, and this distributed process requires multiple nodes interacting in a P2P network. There is *no central unit* responsible for coordinating the node interaction or contracting, which makes the system *trustless*[185]. The distributed feature creates concerns that exist between the liable entities and the possibility to change the governance rules based on specific regulation. This requires *the definition of regulatory boundaries* and protocols for *liability isolation* between the participants.[186]

The conflict exists between the unrestricted freedom to use DLT-based framework peacefully as a constitutionally recognized human right and having limitations of rights where rules and

[185] On the contrary, it can be argued whether DLT is truly a trustless system. Mougayar – Buterin 2016, p. 40 emphasize that blockchain does not eliminate trust but sifts it: trust is always needed, but blockchain *changes how trust is given and how it is earned*. Further, Kasireddy, 2018 argues that blockchains do not eliminate trust but *minimize the amount of trust demanded* from any single party in the system. Trust is distributed between the parties in the system that encourages the parties to co-operate with the rules defined by the system and why blockchain (DLT) is not a truly trustless transactional system.
[186] ITU-T 2019, p. 5.

policies create restraints on DLT usage activities. The key regulatory challenges with property 1 lie with the *applicability of existing law*; *legal responsibility* in multiple jurisdictions; the accomplishment of *interoperability requirements* (the heterogeneity of DLT devices); *new digital forms of law* relating to DAOs and decentralized e-contracting; *protection of secrecy*; cross-border *data localization*; market *competition*; and multi-jurisdiction and *arbitration*.[187] ITU proposes forthcomings in the fields of criminal and civil liability for blockchain distributed control; decentralized managers (human or not); authoritative sources of data; and DLT-record and other related digital sources of legal proof.[188]

The omnipresent nature of DLT poses jurisdictional challenges, which have been discussed previously in this research. Currently, a comprehensive regulatory approach to DLT and blockchain does not exist, and the regulatory approaches are more relating to the features or components of DLT, such as cryptocurrencies.[189] Even if ITU recognizes the jurisdictional challenges and the related issues, the recommendations have disregarded recommendations in relation to the applicable law, which would be highly necessary and leaves the question unanswered.

Autonomy and responsibility (property 2) are strongly linked to *smart contracts* (SC). Transactions on DLT are autonomously executed based on the set conditions, and the legal effects are associated with contract automation. The execution of code should not infringe mandatory laws, but if that happens, the remedies should be set *on-chain* basis (SC self-correction; automated arbitration or other dispute resolution) or *off-chain* (external compensation).[190]

The tool to ensure compliance in the digital environment is the *regulation of information service providers (ISP)* and *information intermediaries*. This includes the limitations of liability of ISPs when they do not affect the network content and taking action to prevent information access by third parties based on legitimate requests from state officials and rights holders. There has been a shift towards regulating the network administrators instead of end users, which requires an establishment of an administrator who creates an information ecosystem around the network

[187] ITU-T 2019, p. 7.
[188] ITU-T 2019, p. 8.
[189] OECD 2018, p. 19.
[190] ITU-T 2019, p. 9.

setting the rules and the participant verification.[191] A more practical solution could be found from the previously introduced model of *Internet information gatekeepers*[192] in order to recognize the actual information gatekeepers since ITU recognizes solely ISPs even if ISPs are just one form of information gatekeepers. Based on the gatekeeper model, gatekeepers are divided into *macro-gatekeepers*, *authority gatekeepers* and *micro-gatekeepers.* The level of responsibility depends on the amount of impact the gatekeeper has.

Agents establishing the organizational and technological rules for networks (such as developers and administrators); agents actively involved in the information and validation of blocks (such as miners); and agents ensuring the use of an electronic platform (facilitators) are recognized into the circle of persons ensuring the operability of DLT network and having the power to impact to its use. The regulation of the actions of these agents is seen as the most effective way to ensure the legitimacy of DLT networks. The regulation should influence *the network administrator,* who retains the ability to influence its development and content. A stricter option would be licensing of activities and creating a controlling system overseeing its implementation.[193]

In addition to network administrators, it is noted that a distributed ledger includes *a software shell* that is an application allowing the interaction between users and the ledger. By providing the ability to use application software between network administrators and its users, there exists a relationship that can be qualified as licensing services or remote access services. Additionally, it seems that the users can be identified and verified on the application software level, which would solve problems of regulating relationships in the information environment since the issues are frequently arising from the distributed nature of the network.[194]

Even if many legal issues with DLT and blockchain are linked to the decentralized nature and the lack of intermediaries, the suggestion of influencing the network administrators seems somewhat the establishment of central authority, which may not be such straightforward. Overregulation is equally a risk to the system as the lack of regulation since overregulation has the potential to destroy the whole innovation. ITU does not consider the differences between public and private blockchain with regard to the regulation of administrators. The private

[191] ITU-T 2019, p. 11.
[192] See Laidlaw 2010, pp. 271–274.
[193] ITU-T 2019, p. 12.
[194] Ibid.

blockchain itself offers a solution since the participants are known and identified. Would the regulation of an administrator in practice mean that the public blockchain would actually become a form of private one since there would be a control system overseeing the implementation? However, it must be noted that broad implementation of public blockchains in practice seems impractical since the lack of identity is not a desired feature in business operations and partnerships.

DLT is *tamper resistance* (property 3), which is based on cryptographic signatures by cryptographic keys; data chaining with cryptographic hashes preventing data modification; and data sharing with users where consensus algorithm synchronizes the stored information. The validity of data is confirmed by signature verification, and the verification process is performed through content signing again and comparing it to a presented signature.[195]

The regulatory challenges are associated with *the correction or removal of data* in the ledger. The central conflicts are recognized with GDPR relating to the right to be forgotten (Art. 17), the right to rectification (Art. 16) and the right to restrict processing (Art. 18). These requirements create a conflict with the immutable nature of DLT. GDPR requires a processing agreement between the data controller and processor and limits the data transfer to third countries. It is unclear how the requirement of processing agreement should be interpreted with public blockchains and with the fact that the nodes in the third countries may transfer personal data to those countries. In addition to GDPR, other laws may require the removal of personal information and non-personal data from the ledger in case of infringement of personal or commercial rights or violation of criminal laws.[196]

ITU proposes *a cryptographic framework standardization* by setting standards but leaving room for the adjustment of algorithms and key lengths without altering the definitions. This would enable the adjustment of the algorithm and use key length. Organizational recommendations include the advice to avoid storing clear-text personal data on blockchains, unless the justification is permanent. Additionally, other security measures such as secret passwords and the performance of risk analysis are requested. However, at this point, recommendations for regulators have not been set yet.[197]

[195] ITU-T 2019, p. 14.
[196] ITU-T 2019, p. 16.
[197] ITU-T 2019, p. 19.

Privacy protection is a matter of public policy, rather than leaving the protection to markets where individuals are activating technological solutions.[198] Privacy issues in relation to DLT are already clearly recognized since the system is currently posing challenges to GDPR compliance. The tamper resistance nature creates issues with regards to deleting incorrect and unnecessary information. Even if the advice on information storage on blockchains would be provided, there is always a risk of human error, which cannot be prevented solely with regulation and prior advice. Mechanisms for data removal from blockchain are especially needed with personal information. Public policy is responsible for ensuring that these mechanisms are implemented. Unfortunately, ITU does not provide any regulatory recommendations with regard to this matter, even if it is already occurring.

Blockchain governance requires *incentive mechanisms* since incentivization has an effect directly on governance (property 4). Presently, economic simulation is the most effective incentivization for permissionless or public DTLs commonly in a *tokenized* format that are transferable and limited in number. For building a valid concept in any jurisdiction globally, multiple legal perspectives should be adopted into a financial system (public law) or via private contracting (private law).[199]

The framework classifies tokens into three categories:

1. Tokens are considered as *cryptocurrencies* if they do not prescribe any right but are tradable;
2. Tokens are considered as *utility tokens* if they can be used as vouchers for a service on or off the chain;
3. Tokens are considered as *asset tokens* if they refer to an asset.

The term *tokenization* is commonly referring to the change of system used for the representation of economic valuable rights. Coin-based tokens should be regulated by central banks in terms of national monetary policy. Asset tokens should be treated as securities, and utility tokens are categorized as securities if they have an investment purpose at the point of issue.[200]

[198] Raab – de Hert 2007, p. 8.
[199] ITU-T 2019, p. 20.
[200] ITU-T 2019, p. 20.

Representation of rights, such as voting rights, incorporated into tokens, such as securities and utilities, is seen as an essential issue that needs national legislators' attention since it concerns the system of creation of credits, their cession and extinction. When connecting tokens to some assets, a new legislation is needed to ensure that buyers acquiring a token in good faith are protected if a prior token transfer was not executed by the authorized holder of the token.[201]

Currently, different states have different approaches for token-based financing methods: a complete ban; regulation based on securities regulation (digital objects are viewed as digital assets); specialized simplified regulation; or no regulation for pure utility tokens. For regulation, a combination of self-organizing, public-administrative and national and international law approaches are needed to regulate the basic blockchain consensus process, smart contract validity in different jurisdictions, optimal regimes to regulate the intermediary actions and the private law asset and security market relating to public law regimes connected to the tokens.[202]

The understanding of the legal nature of cryptocurrencies and tokenization seems to create a challenge for all legislators and other legal professionals since possible lack of technical understanding and also the need for a law to categorize different properties. The categorization of assets is needed, and cryptocurrencies cannot be handled as a whole.

Another issue is with the current financial regulatory system, which is largely based on intermediaries, such as banks, brokers and insurance companies, and the regulation is executed by regulating the intermediaries. Contrary to the traditional system, blockchain is disintermediating these intermediaries, which raises the question of how this traditional system with intermediaries can be shaped to fit in the new financial system without intermediaries.[203] Another fundamental question is whether cryptocurrency can be classified as money or should it be treated through general rules of intangible assets.[204] Or more simplified: "*When money as we know it is around, thinking blockchain is easy. The concept of a token is the confusing part*."[205]

ITU sees incentive mechanisms through economic simulation as the most effective incentivization for permissionless or public DLT. Further, economic incentives should be

[201] Ibid.
[202] ITU-T 2019, p. 21.
[203] OECD 2018, p. 22.
[204] World Bank Group 2020, p. 41.
[205] OECD 2018, p. 24.

merged into the foundation of the systems, which are often in tokenized format involving technical, legal and economic aspects. However, even if the importance of incentive mechanisms is highlighted, it leaves unanswered what these incentives are and how they should be implemented and built into the system.

Even if transparency and openness are considered as positive features of DLT by making it more secure, these features cause some challenges (property 5). The challenge is that the information in the ledger is transparent for everyone, but it is also private, which will ensure the anonymity of participants in a certain transaction. *The right balance between transparency and privacy* is central for DLT to comply with regulation and other norms. As an example, also mentioned earlier, the DLT imposes a contradiction with GDPR that provides control over personal information and the right to be forgotten. Additionally, full transparency causes challenges to some business models such as the banking sector and effects on the competitive advantages generally because the full disclosure of the information would reveal the investment and business strategies and people involved in these.[206]

ITU recommends that DLT protocols and governance adjust the level of openness and transparency in accordance with regulation and recognizing the particular features of different sectors. On an *off-chain* approach, the information could be stored in access-controlled private storage where the information can be deleted afterwards. On-chain information encryption is not recommended since the immutable nature of the information.[207]

Claiming that full transparency causes challenges only *to some business models,* such as the banking sector, is somewhat peculiar. In concrete, does any business operating party seek full transparency even if there is no binding regulation towards the opposite? With regard to business operations, the commonly recognized fact is that it involves business plans that are not public for everyone. Based on this, the use of public blockchain seems quite problematic. Is it actually able to offer better benefits that do not yet exist, and is it worth taking the risk of unintended information exposure? *Schneier* illustrates the underlying issue with blockchains:

[206] ITU-T 2019, p. 24.
[207] ITU-T 2019, p. 25.

> *"What blockchain does is shift some of the trust in people and institutions to trust in technology. You need to trust the cryptography, the protocols, the software, the computers and the network. And you need to trust them absolutely, because they're often single points of failure."*[208]

The underlying issue with blockchains is that essentially, we are talking about codes that may have bugs or errors, or the system can get hacked. Is this system truly reliable in storing confidential or personal information since, ultimately, the exposure of this kind of information is likely worse than the benefits achieved with transparency?

One approach to resolve cross-border Internet policy conflicts can be called *universalism,* according to which all states should try to control the Internet, but mostly the application of universal rules is not possible for the Internet policy since the states differ much in their values and approaches. An opposite approach is to grant each state the freedom to implement their own Internet policies as they wish, which seems to be the more dominant approach at the moment. However, the issue with this approach is that the decisions of one state can have an impact on other states, individuals and businesses outside the borders of that state which may not be taken into account.[209] This leaves the role of international organizations in the establishment of an international regulatory framework for blockchain unclear. The international harmonization of blockchain regulation seems quite unrealistic since the differences between the states, even if the need for harmonization can be recognized. Anyhow, focusing on the two opposite ends may not result in any solutions. Instead of trying to universalize the regulation or leaving it completely on the national level and to the discretion of individual states, a middle ground should be sought. International organizations serve as a forum for international co-operation and discussions.

ITU proposes recommendations with regard to blockchain regulation which ultimately leaves the execution on the national level. On the other hand, according to ITU, the framework provides practical recommendations for users, regulators and technologists in order to mitigate the possible risks with DLT.[210] However, partly the framework is mostly focusing on recognizing the regulatory issues that DLT, and blockchain and its features, are causing, which have already been mentioned in academic literature, such as distribution, decentralization, autonomy, tamper resistance and transparency. Additionally, the framework promises practical

[208] Schneier 2019.
[209] Castro – Atkinson 2014, p. 10.
[210] ITU-T 2019, p. 3.

recommendations, which are partly questionable since there are no recommendations given to property 3, and some of the recommendations are listed in brief bullet points. The level of practicality and comprehensiveness could be improved.

ITU framework is a development of new regulation for blockchain technology, and it has had the opportunity to comprehensively take the blockchain features into consideration. It is recognized that private actors have a role in blockchain, and the system is not tried to forcibly put under public control. The approach seems to be more co-operative between public and private actors. Nevertheless, this approach may not necessarily promote technological determinism, but could the recognition of the role of private actors in blockchain technology present a form of soft expression of technological determinism?

3.4.2 UNCITRAL Model Laws

The United Nations Commission on International Trade Law (UNCITAL) is a legal body functioning under the UN in the field of international trade law. UNCITRAL's purpose is to harmonize and modernize the rules on international business.[211] UNCITRAL has issued model laws with regard to electronic commerce: *The Model Law on Electronic Commerce (1996), The Model Law on Electronic Signatures (2001), The Convention on the Use of Electronic Communications in International Contracts (2005), The Model Law on Electronic Transferable Records (2017)* and *The Model Law on Secured Transactions (2019).* The purpose is not to analyze all of them comprehensively but to seek represented solutions that could be adapted to blockchains. There are two recognized pathways towards international blockchain regulation, which are the adaptation of current legislation to blockchains or passing new laws. The purpose of this chapter is to research the first mentioned by seeking the possibilities to adapt existing UNCITRAL model laws to blockchain technology.

Under *the Model Law on Electronic Commerce* (EC Model Law), *a legal effect* cannot be denied to information only based on the form of the data message.[212] In the context of contracting an offer and an acceptance can be expressed by means of data messages, and the validity or enforceability cannot be denied on the grounds that a data message was used for the purpose.[213] In appropriate situations, the states may, under their legal systems, extend this by

[211] United Nations Commission on International Trade Law 2020.
[212] UNCITRAL Model Law on Electronic Commerce 1996, Art. 5 and 9.
[213] Ibid. Art. 11

providing that the contract performance by an automated system cannot be denied the effect based on that the actions were executed by an automated system.[214] This could provide clarity to the discussion around the validity of smart contracts. EC Model Law defines the conditions that a data message must meet to be able to fulfil the purposes and functions of paper-based document requirements of writing and a signature.[215] The EC Model Law additionally requires a reliable assurance of the integrity of the information stored in the data message before the information is seen to satisfy the presentation of the original form required from the paper-based documents.[216]

According to Article 12 of *the Convention on the Use of Electronic Communications in International Contracts*: "A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract." This could provide some clarity with regard to the validity of smart contracts and blockchain transactions, even if the functioning of smart contracts has faced criticism.[217] Solving the issue around the validity discussion would allow the adaptation process to evolve since, as far as it is unclear whether smart contracts are valid, the progress of regulative adaption and legislation process is at a standstill. However, validity is just one of the many recognized legal issues around smart contracts.

The Model Law on Electronic Transferable Records (ETR Model Law) declares that an electronic transferable record shall not be denied legal effect, validity and enforceability solely on the basis that it is in electronic form.[218] ETR Model Law sets conditions under which an electronic record is to be treated as a transferable document, such as bills of lading and warehouse receipts. ETR Model Law is relying on the principle of functional equivalence by defining the conditions that must be met in order for the electronic transferable record to become an equivalent to paper-based record.[219] The electronic transferable record could serve as a smart contract, for example, a promissory note could be coded as a smart contract: when the

[214] Takahashi 2017, p. 3.
[215] UNCITRAL Model Law on Electronic Commerce 1996, Art. 6–7.
[216] Ibid. Art. 8.
[217] As an example, see Werbach – Cornell 2017, pp. 365–374. There exist uncertainties in the contractual areas such as meeting of the minds, consideration, capacity, legality, enforcement and restitution.
[218] UNCITRAL Model Law on Electronic Transferable Records 2017, Art. 7.
[219] Ibid. Art. 10.

timestamp reaches the expiration rate, the automatic execution of a smart contract would occur, and the payment would automatically be executed from the issuer to the holder.[220] However, it must be noted that ETR Model Law is not applicable to cryptocurrencies since the holder of cryptocurrencies has no right to claim performance from anybody since the value is based on the willingness of the participants in the blockchain to accept them as a means of payment.[221]

Another recognized challenge with electronic transferable records is the prevention of singularity since the law commonly requires an original copy of the transferable document in the circulation. ETR Model Law attempts to provide functional equivalence to this issue by setting the requirements for electronic transferable record to meet:

a) The electronic record contains the information that would be required to be contained in a transferable document or instrument; and
b) A reliable method is used:
   i. *To identify* that electronic record as the electronic transferable record;
   ii. To render that electronic record capable of being subject *to control* from its creation until it ceases to have any effect or validity; and
   iii. To retain the *integrity* of that electronic record.[222]

This provides two approaches: singularity (i) and control (ii), but this does not automatically mean that the approach is capable of solving the problem of uniqueness. Since everyone in the network has a copy of the record, singularity and control under ETR Model Law would be challenging to achieve.[223] Conventionally, there exists an administrator of a registry functioning as a trusted party ensuring that the records are under the exclusive control of their holders, but the blockchain technology is able to replace such administrator with an algorithm securing the true versions of distributed ledgers and ensuring that the records are under the exclusive control of their holders, meaning the holder of the private keys.[224]

According to Article 2 of ETR Model Law, an electronic record includes *all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not.* Even if the copies of one record are saved in the

[220] Ng 2018.
[221] Takahashi 2017, p. 5.
[222] UNCITRAL Model Law on Electronic Transferable Records 2017, Art. 10.
[223] Ng 2018.
[224] Takahashi 2017, p. 5.

computers of the blockchain network, this would not prevent the recognition as an electronic record under ETR Model Law. As an example, even if there are copies of electronic transferable records in participating computers, at any given time, the specific record and its owner can be identified and the information verified. This may provide the solution to the issue of singularity and control.[225] It is recognized that uniqueness poses technical challenges in an online environment, and an absolute guarantee of non-replicability may not be technically possible. Furthermore, the use of paper documents has provided information on the associated risks in relation to their use, while these practices associated with the use of electronic transferable records are not yet well enough established.[226] However, there always exist other kinds of challenges in relation to security compared with paper-based documents, such as hacking the private key or disclosure by accident. Though, previously discussed sandboxing strategy could provide safe grounds for testing reliable methods *ex ante*.

UNCITRAL Model Law on Secured Transactions (ST Model Law) classifies assets into four categories:

> A security right may encumber:
>
> a) Any type of movable asset;
> b) A part of or an undivided right in a movable asset;
> c) A generic category of movable assets; and
> d) All of a grantor's movable assets.[227]

Takahashi divides blockchain-based assets into four categories: (1) receivables denominated in a cryptocurrency; (2) the units of cryptocurrencies; (3) blockchain-based tokens representing negotiable documents; and (4) blockchain-based tokens representing securities.[228]

According to Article 1 of ST Model Law, the law is applicable to security rights in movable assets. Furthermore, *a secured transaction* means a transaction that creates a security right in a movable asset and *movable assets* are defined as tangible or intangible assets, other than immovable properties. The rules contained in the ST Model Law would be applicable to a receivable denominated in a cryptocurrency.[229] Since the cryptocurrency does not meet the

[225] Ng 2018.
[226] UNCITRAL Model Law on Electronic Transferable Records 2017, daft explanatory notes para. 82.
[227] UNCITRAL Model Law on Secured Transactions 2019, Art. 8.
[228] Takahashi 2017, p. 7.
[229] Ibid.

definition of money[230], its classification could be considered as a right to payment of funds credited to a bank account.[231] ST Model Law defines a *bank account* as an account maintained by an authorized deposit-taking institution to which funds may be credited or debited, and *receivable* as a right to payment of a monetary obligation, excluding a right to payment evidenced by a negotiable instrument, a right to payment of funds credited to a bank account and a right to payment under non-intermediate security.[232] In order for cryptocurrencies to be classified as funds under ST Model law, they should be maintained in the form of an account and by an authorized deposit-taking institution.[233] Within broad non-technical interpretation, an online wallet provider could qualify as an authorized deposit-taking institution where it is authorized by law to receive the deposit of cryptocurrencies.[234]

According to Article 8 of ST Model Law, a security right may encumber any type of movable asset. *Units of cryptocurrency*[235] can be considered as movable assets as a tangible or intangible asset other than immovable property as defined in Article 2(u). Further, according to Article 6(1), the creation of a security right requires a written agreement, unless the secured creditor is in the possession of the collateral, identifying the secured creditor and grantor, and moderately describes the secured obligation and the encumbered asset. The described general requirements of the collateral in the security agreement and registered notice would apply to digital assets. However, the digital assets must be identified, and collateral can be described as "all assets", "all digital assets", or "all cryptocurrencies".[236]

According to Article 2(ll) of ST Model Law, *negotiable documents* are considered as tangible assets. However, electronic negotiable documents, including blockchain-based tokens representing negotiable documents, belong to the category of intangible assets as defined in Article 2(p) as any movable asset other than a tangible asset. However, the ST Model Law does not provide specific rules applicable to electronic negotiable documents.[237] Practically, there is no use to establish a security right in an electronic negotiable document unless it is extended,

[230] *Money* is defined as currency authorized as legal tender by any state. See Art. 2(e) of UNCITRAL Model Law on Secured Transactions 2019.
[231] World Bank Group 2020, p. 24.
[232] UNCITRAL Model Law on Secured Transactions 2019, Art. 2(c) and (dd).
[233] World Bank Group 2020, p. 24.
[234] Takahashi 2017, p. 8.
[235] Takahashi 2017, p. 8 considers security rights in cryptocurrency units themselves rather than in a receivable denominated in a cryptocurrency.
[236] World Bank Group 2020, p. 26.
[237] World Bank Group 2020, p. 22.

under the applicable law, to the tangible asset covered by the negotiable document. In order to avoid these problems, the state may extend the application of the rules for negotiable documents to electronic negotiable documents.[238]

In Article 2(w) of ST Model Law, *non-intermediated securities* are securities other than those credited to a securities account. Further, according to Article 2(ii) *securities account* is an account maintained by an intermediary to which securities may be credited or debited. A blockchain could make it possible to trade securities based on a peer-to-peer (P2P) network and hold those without the participation of a trusted intermediary. Blockchain-based tokens enacting securities, crypto securities, would thereby be considered as non-intermediated securities.[239] However, laws would have to be amended to superimpose negotiability on digital assets in order for them to become functional equivalents of investment property, for example.[240]

Another discussion around blockchain-based securities is whether a distributed-ledger platform can serve as a *registry* since the registration of a notice in the registry renders the effective security right against third parties.[241] A permissioned DLT system could serve as a registry since the permissioned system allows the registry operator to determine the readability of the ledger only to certain nodes, and only authorized nodes can submit and validate new data blocks.[242] Ultimately, the enacting state is responsible for the operation of the registry; thereby, the use of public blockchains is not an option since they are not controlled by any specific authority.[243] Additionally, with permissioned blockchains, the consensus algorithm can be designed to control that the registrations are added in the order of submissions.[244] As a result, it seems that a permissioned blockchain could serve as a registry.

UNCITRAL Model Laws provide at least some baseline clarity to smart contracts and the treatment of cryptocurrencies. A discussion around smart contracts questions if they are even valid contracts. With UNCITRAL Model Laws, it could be established that smart contract can be valid contracts and enable to focus more on the other legal issues with smart contracts, such

[238] Takahashi 2017, p. 10.
[239] Takahashi 2017, p. 11.
[240] World Bank Group 2020, p. 28.
[241] UNCITRAL Model Law on Secured Transactions 2019, Art. 18.
[242] World Bank Group 2020, p. 14.
[243] Takahashi 2017, p. 12.
[244] World Bank Group 2020, p. 14.

as immutability, automated execution and interpretation, and seek whether these issues can be solved with further development that requires co-operation between the states and between the technologists and legal professionals. By stopping at the validity discussion, it risks the underlying potential of smart contracts without further exploring the possibilities. It is commonly sought for positive outcomes and prevented the negative ones by regulating a certain issue. New technology regulation has a high impact on the development by establishing a proper framework or with overregulation destroying the whole innovation. Therefore, a more deliberate approach could be via the existing regulation. Additionally, it must be kept in mind that blockchain technology is not the first great technological innovation that the law has faced, and it should be approached with more discretion since the correct regulatory solutions have been discovered before with the World Wide Web as an example.

The essential clarification that UNCITRAL Model Laws provide with cryptocurrencies is with their treatment, not as money but other kinds of assets. Until now, cryptocurrencies have been the largest blockchain application facing the highly regulated financial sector. Additionally, it seems that the development should be taken towards private blockchains since the public blockchains cause multiple legal challenges such as privacy issues and lack of control.

However, UNCITRAL Model Laws appear to provide some clarity with only two blockchain applications while still leaving unsolved questions and not providing more comprehensive solutions. There exists a wide range of potential blockchain use cases[245] than solely smart contracts and cryptocurrencies. Even if the approach through existing regulation could be more delicate and offer the baseline for regulatory development, the issue with existing regulation may be that no legal framework comprehensive enough exists for blockchain technology. UNCITRAL Model Laws seem to present a more traditional approach to law-making by a central authority and do not consider technology itself as a changing force in the society which does not illustrate technological determinism much.

[245] See Business Insider Intelligence 2020.

4 BUILDING INTERNATIONAL REGULATORY GOVERNANCE

4.1 International Co-operation

4.1.1 Global Public Administration

As discussed in previous chapters, blockchain challenges the traditional understanding of state jurisdiction, and due to the global nature of the technology, it spreads under several jurisdictions causing challenges to define the applicable law. Additionally, it seems that blockchain has developed its own so-called own jurisdiction by creating a society around the technology, which it is able to courage to behave in desired ways for the blockchain community. The legislative field struggles with different strategies and approaches to regulating blockchain technology, but moreover, the public international law has met a situation where the rule creation has begun to develop on a private law-like level without the democratic legitimacy of public law-making.

> *"Governments, as well as the private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centered Information Society is a joint effort which requires cooperation and partnership among all stakeholders.*
>
> *We aim at making full use of the opportunities offered by ICTs in our efforts to reach the internationally agreed development goals, including those contained in the Millennium Declaration, and to uphold the key principles set forth in this Declaration. The Information Society is intrinsically global in nature and national efforts need to be supported by effective international and regional cooperation among governments, the private sector, civil society and other stakeholders, including the international financial institutions."* [246]

The establishment of cross-border *public administration* that would take the jurisdictional challenges into account could be a building component of the above-mentioned Information Society. The above Declaration of Principles Building the Information Society: a global challenge in the new Millennium invites public and private parties together to create a global information society that requires the co-operation of different stakeholders.[247]

[246] World Summit on the Information Society 2003, para. 20, 60.
[247] Melnyk – Barikova 2019, p. 75.

Such a partnership between the parties of society, public and private, could reflect the interests of public administration and private entities. Based on this, it could be possible to create a system of public administration that would, in addition to legal framework, take into consideration the evolving trends in the society that are occurring due to technological innovations, for example.[248]

However, even if the discussion is mostly divided into two separate parallel worlds, cyberspace and the physical world, blockchain and the physical world do not solely operate in isolation from each other. The challenges that globalization has posed to the legal governance of blockchain technology are not necessarily issues of hybridity but rather issues of *interoperability* of these different systems between different private actors, and between public and private actors. The new framework for blockchain must take into consideration the functioning of interoperability between the cyberworld and physical world, such as the access points, intermediaries, for example, between these worlds.[249]

4.1.2 Autonomous Code-based Communities – Are They Outlaws?

The legal or non-legal nature of autonomous legal systems developed by private parties without public democratic legitimation was previously introduced with Lex Mercatoria. Blockchain is additionally challenging the understanding of the legal system and law-making by being able to establish a system parallel to the traditional legal system, which has the ability to develop rules that the community is obeying. This raises the question of what law by nature actually is if private actors can create a similar norm system that has been understood and legitimized as the functions of public law? On what grounds it can be said that something is law or is not law?

> *"Law is about text, or should we admit – more precisely – that law exists as text? If the latter is true, should we expect that artificial intelligence – as a technology – transforms the mode of existence of the law?"* [250]

It can be stated that law can exist as a tool for social planning since ruling by law is essentially a rule of man by way of law, which brings subjects to the law under the will of the ruler. However, the *rule of law* can be additionally defined as the system that brings legislators and

[248] Melnyk – Barikova 2019, p. 76.
[249] Dimitropoulos 2020, p. 1191.
[250] Hildebrandt 2015, p. 161.

the administration under the jurisdiction of the law. If a law is neutral, the adherence to the rule of law is not necessary, but within the context of the rule of law, a law is defined as a set of norms that are part of the rule of law.[251] Broadly, there are two opposite viewpoints regarding the nature of blockchain technology as law or more clearly as autonomous legal system. Technological determinism views law neutral, and sees it as a separate legal system, such as presented with Lex Informatica and Lex Cryptocraphia. However, this is problematic from a public law perspective since public law and its legitimacy is linked to the rule of law and the constitution of a nation state.

4.1.3 International Harmonization

The national level regulations may be overlapping and conflicting with each other. As an example, from multinational companies' perspective by conducting business in several jurisdictions means being subject to these jurisdictions and the possible conflicting laws and regulations these jurisdictions may have with each other.[252] The lack of international harmonization has been identified as a challenge, especially in the financial sector, since the varying regulatory requirements increase the complexity and costs of compliance.[253] The DLT may have the potential to minimize documentary fraud and help to create international regulatory standards and decrease costs.[254] The benefits of international harmonization are for multinational companies to implement global operating standards uniformly, which saves costs and enables more efficient operation.[255] It is argued that in order to support innovation, economic growth and jobs, the blockchain ecosystem as a whole, with entrepreneurs, corporation and developers, is dependent on predictable, relevant and understandable regulation.[256]

It is noted that the lack of effective and harmonized policies and regulation may lead to the rise of *Blockchain Havens,* which is an example of a possible negative outcome. The blockchain havens are jurisdictions attracting blockchain entrepreneurs by offering shelter from tax and regulation. Due to the highly anonymous and self-regulated nature, blockchain is able to offer illicit users the typical benefits of tax havens, such as lack of transparency and information

[251] Hildebrandt 2015, p. 164.
[252] Ko 2012, p.14.
[253] International Chamber of Commerce (ICC) 2017, p. 105–108.
[254] International Bar Association (IBA) 2017, p. 34.
[255] Marchant – Abbott 2013, p. 395.
[256] The European Union Blockchain Observatory & Forum 2019, p.10.

exchange. The blockchain haven is able to independently offer an unregulated start point for illicit blockchain applications.[257] International harmonization may prevent the birth of blockchain havens in which certain jurisdictions may try to attract business operations by offering looser regulation.[258] Individual jurisdiction may pose problems to global welfare since the local assessments of regulatory impacts would not necessarily consider ramifications outside their national jurisdictional boundaries.[259] Additionally, there exists a risk of over-regulation when several regulators exercise jurisdictions over the same business operations.[260] While recognizing the need for coordinated international efforts for preventing the possible regulatory race at the same time acknowledging the fact that this has not comprehensively succeeded with tax havens, and raising the question if international regulation has not been able to eliminate tax havens, how is it able to prevent blockchain havens? However, the blockchain phenomenon is somewhat novel compared to tax havens, and the effective approaches taken before the development of premature features towards blockchain havens could have a better possibility to operate effectively.

While considering the inadequate harmonization from an international perspective, there are troublesome situations between the larger and smaller jurisdictions. As an example, the EU and the United States are two significant jurisdictions with active enforcement and partially overlapping jurisdictions on several issues. The smaller jurisdictions and the companies operating there are somewhat underdogs without an opportunity but to comply with the applicable regulations or withdraw the business in the jurisdiction in question: companies in smaller jurisdictions are not able to benefit from regulatory havens. [261]

Even if the benefits of international harmonization could be recognized and justified, there are still viewpoints against international harmonization. Harmonized or uniform regulation may not be desirable while considering the differences between the states in public perception, economic standing, industrial strengths and regulatory frameworks.[262] The co-operation may be challenging to achieve, enforce and sustain, and it may generate an additional bureaucracy layer between the citizens and decision makers.[263] Another challenge for adopting international

[257] Marian 2019, p. 31.
[258] Ibid.
[259] Ko 2012, p.14.
[260] Ko 2012, p.18.
[261] Ko 2012, p.18.
[262] Marchant – Abbott 2013, p. 396.
[263] Guzman 2002, p. 272.

harmonization may be the current adoption of wait-and-see -strategy and the lack of proper legislative initiatives on an international level. The national level regulation is more efficient in constantly evolving while international organizations and international co-operation is more staying on the level of naming and recognizing the issues caused by DLT. Another challenge is the preferred approach to use non-legally binding instruments on international regulation, which raises the question of whether these non-binding recommendations, model laws and best practices are sufficient enough to produce effective harmonization?

4.1.4 International Regulatory Co-operation

International regulatory co-operation (IRC) is for helping governments to achieve policy goals and minimize costs. Additionally, regulatory co-operation can provide solutions for transnational market failures, trade barriers and other cross-border challenges. The role of international organizations is to facilitate the development of shared language and the comparability of policies and approaches. For states to develop international legal and policy standards, international organizations, as an example of one forum, provide an institutional framework and technical expertise.[264]

For promoting IRC, there exists instruments in three categories: (1) Legally binding instruments, such as convention and treaties, agreements and decisions; (2) non-legally binding instruments, such as recommendations, model laws, technical standards and best practices; (3) non-legally binding instruments with a statement of intent, such as (political) declarations, policies and guidelines.[265] Based on the OECD's survey, *non-legally binding instruments are much more frequently used than legally binding ones*.[266] Most implementation instruments encouraged by international organizations are soft tools such as progress benchmarking, peer review and positive incentives for implementation. Formal instruments such as dispute settlement and sanctions are less frequently used. These reflect the limited use of legally binding instruments of international organizations and that the non-legally binding instruments are used more often.[267] The fact that non-legally binding instruments are commonly used among the soft implementation tools seem to leave much discretion on a national level. The scale is not well

[264] OECD 2016, p. 5. On the contrary, Guzman 2002, p. 272, presents that seeking strategies that require as little co-operation as possible is preferable and effective international regulation can be achieved by low level of co-operation by regulating only the choice of law rules.
[265] OECD 2016, p. 58.
[266] OECD 2016, p. 60.
[267] OECD 2016, p. 74.

balanced, and international organizations could take more responsibility and more binding actions towards legally binding harmonization while still leaving room for specific implementation on a national level. There exists a slight contradiction between the recognized need for harmonization and the concrete actions taken towards it.

Ko divides international harmonization and co-operation into three different categories: soft co-operation, procedural co-operation and substantive harmonization. *Soft co-operation* is based on sharing information on technical expertise and investigative methods that would be helpful for regulators. The essential limitation of soft co-operation is that it is voluntary, and the actual co-operation depends on the self-interest of participants.[268] *Procedural co-operation* takes a step further by facilitating international co-operation at the enforcement level.[269] The establishment of choice of law rules would certainly bring clarity on the omnipresent jurisdictional challenges in relation to blockchains. *Substantive harmonization* would eliminate issues arising from lack of legislation, and the problem of overlapping jurisdictions could be avoided. This would require the measures to reach multijurisdictional consensus, preparation of an international convention and measures to harmonize national laws and regulations themselves.[270] To actually reach the recognized need for harmonization, the procedural co-operation seems to set the minimum level. Soft co-operation may not be sufficient enough to resolve the international phenomena effectively in relation to blockchain technology that greatly poses jurisdictional challenges with regard to applicable jurisdiction, reaching criminal liability and enforcement. The co-operative goals and harmonization need the initiatives and coordination from international organizations to save costs but to actually implement international level regulation since it is not necessarily the primary interest of national authorities.

An effective way would be to regulate technology via a formal international treaty or similar intergovernmental agreement containing essential regulatory commitments. Possibly a more practical approach could be a coordinated framework that would include an intergovernmental agreement establishing an annual conference for monitoring development.[271]

[268] Ko 2012, p. 21.
[269] Ko 2012, p. 22.
[270] Ko 2012, p. 26.
[271] Marchant – Abbott 2013, p. 393.

Even if the goal is towards international harmonization, the fact that states will inevitably create their own blockchain regulations, which will conflict, must be admitted. *The International Technology and Innovation Foundation (ITIF)* has developed a framework for cross-border Internet policy which can be applied to blockchain technologies for resolving conflicting issues. If the issue contains a multinational blockchain's technical architecture, the states should trust the work within existing international entities to change its global functions. If the issue affects parties outside the state's borders, the states should seek to establish formal international agreements on the matter and investigate if the policy conflicts with international agreements.[272]

A somewhat more modest approach towards international harmonization would include coordination between regulatory agencies from different states rather than national governments. Agencies would first agree on the coordinated regulatory requirements and then represent those requirements into their national regulations. Frequently the least rigorous approaches towards international harmonization are the most common ones. It includes regulators meeting from different states, and such interactions are not intended to produce a common regulatory framework. However, these efforts may lead to frustrated regulatory development on a national level that may cause states to pursue their own regulatory direction.[273]

4.2 Emergence of Integrated Global Governance

4.2.1 New Forms of Governance

Blockchain technology illustrates the concept of *social technology,* which includes the ways to communicate, co-operate, compromise and make consensus with other people. It has an impact on the structure of society, systems, interactions between individuals and social relations. Blockchain has the potential to change social organization since it is able to replace the existing social technologies (such as email, messages and other messengers), including *bureaucracy* which, is the most dominant form of organization in modern society.[274]

Blockchain technology has introduced a new way to interact and make transactions that seem to be somewhat out of scope from our traditional legal systems to understand and cover through

[272] Information Technology and Innovation Foundation 2019.
[273] Marchant – Abbott 2013, p. 397.
[274] Jun 2018, pp. 2–4.

traditional governance approaches, which is commonly state-oriented regulation. However, blockchain technology features, such as *decentralization, immutability, external trust and absence of intermediaries,* raise the question of whether it is even possible to approach this through traditional governance since the governance in political science is very different to the governance of networks.

The "old" governance means the governance that is executed primarily through the hierarchical command-and-control state structures and public hierarchies. The system is relying on the institutions in authority setting the policies via the enforcement of hard law. In the old model, the state is legitimate and sovereign in commanding and controlling both private and public actors. In this *identity-based* governance model, the identity of the state is seen as the source of law and policy and an authoritative and legitimate public body acting sovereign over its territory. The authority is delegated from the state to intermediary institutions to perform governance roles. The "new" governance moves away from the vertical command-and-control governance towards more horizontal policymaking. In *the role-based* governance, the tasks are performed by the actors based on the role they can perform to achieve the desired goal.[275]

The distributed nature of blockchain enables distributed registration of documents and asset transactions, which challenges the traditional roles of public administrations and promote the appearance of new governance roles.[276] It is argued that blockchain technology cannot be governed properly through the old governance modes since the power relationships are neither horizontal nor vertical, and the functioning of traditional governance models rely on trust, which blockchain is centrally lacking.[277] The governance system of blockchain and other networks can be said to consist of two parts: *social governance* and *algorithmic administration of governance*. Social governance refers to the human decision-making and institutionalized decision-making process of how the necessary information is received in order to make future protocol updates. The algorithmic administration of governance means the protocol rules written in the code, which are automatically enforced by the computer network.[278]

An option for blockchain governance is *a polycentric governance* that would respect the underlying hacker ethics that highlight the need to better negotiation between individuals and

[275] Zwitter – Hazenberg 2020, pp. 4–5.
[276] Ølnes – Ubacht – Janssen 2017, p. 361.
[277] Zwitter – Hazenberg 2020, p. 6.
[278] Voshmgir 2020

institutions, decentralization, creativity, curiosity, distribution, sharing, transparency and commonality.[279] Overall the governments could pursue to sustain order on the blockchain by shaping the established social norms within the blockchain community.[280] The power relationships of the network must be recognized and understood in specific terms to every network.[281]

Blockchain could transform traditional governance into *network governance* in which various parties are responsible for transacting and governing. Blockchain is able to allow direct interaction between citizens and provide administration without a government administration.[282] The power must be designed as evolving since different parties perform different governance roles in different circumstances. The exercise of power is not center-oriented anymore, which requires new governance modes.[283]

Castells discovers that there are four forms of power especially related to networks: *networking power, network power, networked power, and network-making power.* Every form of these powers specifies certain processes of exercising power. *Networking power (1)* means the power of the actors and institutions included in the networks constituting the core of the global network society over individuals who are not part of these global networks. *Network power (2)* refers to the power resulting from the required standards to coordinate interactions, which is primarily concerning the placement of rules in the network. *Networked power (3)* is the power that different actors have over others within the network, imitating the traditional power concepts, but the way it is used varies per network. *Network-making power (4)* refers to a power of an actor or institution to model or re-program a network according to its interests and values.[284]

The designers of blockchain network search to incentivize good behavior by actors in order to reach the objectives of governance and to reduce the risk of non-compliance with regulation by the network. The compliance could be ensured through regulation by building it into the network, such as locking actors out of the network.[285] The application of traditional governance models threatens to weaken the benefits of technological innovations such as blockchain.

[279] Korhonen – Ala-Ruona 2018, p. 10.
[280] De Filippi 2018, p. 187.
[281] Castells 2013, p. 46.
[282] Ølnes – Ubacht – Janssen 2017, p. 362.
[283] Zwitter – Hazenberg 2020, p. 6.
[284] Castells 2013, pp. 42–45.
[285] Salmon – Myers 2019, p. 7.

Overregulation or application of improper mechanisms reduces the possible benefits of blockchain technology.[286] For regulators, it is necessary to work together with the industry to ensure compliance and allowing flexibility in order to reach the full potential of blockchain systems.[287]

The common feature seems to be that the current governance modes are not proper and sufficient enough to meet the need of blockchain networks. The novel decentralized system requires new approaches which may have the potential to alter our understanding of governance, safe costs, offer flexibility and individual freedom. However, there exists a risk of fraudulent behavior that requires governance outside the network. Ultimately the most challenging question may be how to find a proper regulatory approach without destroying the new technological innovation?

4.2.2 Future Transnational Governance

Transnational governance refers to a concept of international collaboration among public and private parties that is non-traditional and differs from the governance of constitutional states. These possibly less formal arrangements connect technological, economic, and scientific areas with political and legal processes.[288] *Backer* introduces a system of *metagovernance* that is formed via institutional communication for structuring the set of governance subsystems. These subsystems have a private governance host system, such as multinational corporation maintaining their supply system via contractual relationships, global governance frameworks for private governance, and autonomous corporate constitutionalism.[289]

Further, *corporate governance* refers to a management system used for directing and controlling companies. Commonly this is additionally linked to the protection of shareholders from managerial discretion. The underlying idea is that multinational corporations have become so large that they have the power to allocate resources, which means that they have enough power to impact the behavior of others.[290] Even if corporate governance is originally developed

[286] Zwitter – Hazenberg 2020, p. 7.
[287] Salmon – Myers 2019, p. 6.
[288] Joerges – Sand – Teubner 2004, foreword i.
[289] Catá Backer 2011, p. 758.
[290] Daluwathumullagamage – Sims 2020, p. 3. See also Euteiner 2007, p. 765 according to which multinational corporations account for more than one third of the global economies.

for private multinational corporations, it does not mean that institutional structures are not necessary:

> *"To ensure an effective corporate governance framework, it is necessary that an appropriate and effective legal, regulatory and institutional foundation is established upon which all market participants can rely in establishing their private contractual relations."* [291]

The term *governance* is used with different meanings, but within the context of networks and technology systems, it is understood as organizational and economic coordination utilizing decision rights, incentives, and accountabilities. With blockchain, the decision-making rights are based on network consensus.[292] The aspect of social coordination is related to the issue of *trust* that blockchain is implementing by combining informal interpersonal relations, formal rules, and technical solutions.[293] It is to be noted that blockchain has its origins in *open-source software* (OSS), which governance is open and marked by no central authority. OSS has been a foundation in technological development in a number of systems (such as Linux), bringing together groups with shared interests and values for the common good.[294]

Blockchain poses specific governance elements due to its on-chain governance structures, and in an ideal situation, blockchain could be similar to a notion of a positivist legal order. However, in times of crisis, governance structures off-chain may closely remind political governance outside of the legal order that the blockchain itself represents, but still, it is a governance solution based on the structure of blockchain.[295] Decentralized networks, like blockchain, have been associated with the elimination of a single point of power control and offering a solution to govern without governments. However, there exists a variation within the blockchain governance: one end represents the cyber libertarian dream aiming at reducing governmental control, but on the other hand, blockchain could offer a solution for greater social justice by undermining anti-democratic governmental and capitalistic agreements favoring economic inequalities.[296]

The governance frameworks of private entities must be observed and especially the ones developed at the supranational level, since the public governance in the twenty-first century is

[291] OECD 2004, p. 29.
[292] Ziolkowski – Miscione – Schwabe 2020, p. 320.
[293] De Filippi – Loveluck 2016, p. 9.
[294] Ziolkowski – Miscione – Schwabe 2020, p. 320.
[295] Zwitter – Hazenberg 2020, p. 8.
[296] De Filippi – Loveluck 2016, p. 3.

absorbing the characteristics of transnational corporate governance.[297] The blockchain community is increasing the awareness of the shortcomings associated with *code is law* either by pushing the code is law framework further or formal control in the form of off-chain governance bodies (e.g., foundations, consortia) needs to be established.[298]

The options of forming the governance system around blockchain are varying, taking into account their subjectivity to change over time. The decision rights are difficult to assign, and it is not explored which decisions are left to blockchains themselves and which actors or organizations are the ones guiding the development of blockchain systems.[299] The idea of public governance of blockchains is somewhat in contradiction with the origin of the system, which was developed for the common good and apart from the central authorities. However, it seems that the traditional ways of public governance are not operable around blockchain, and public governance must absorb features from private governance systems such as corporate governance.

[297] Catá Backer 2011, p. 757.
[298] Ziolkowski – Miscione – Schwabe 2020, p. 320.
[299] Ibid.

5 CONCLUDING OBSERVATIONS

Technological development, together with globalization, has challenged the traditional understandings of jurisdiction, legislative power, and regulatory governance. The significance of transnational private actors has increased, and this is challenging the role of a nation state as the basis of democracy and legislative authority. Blockchain technology is based on a decentralized ledger, and the network can spread into multiple locations around the world, which is posing jurisdictional challenges and confusions over applicable laws. The need for regulatory harmonization is recognized, but another issue is how to regulate blockchain technology since this requires the understanding of the technical structure and features of blockchain. However, harmonization is not the only regulatory option and may not be the most proper regulatory solution after all, but better co-operation between public and private parties in order to establish a regulatory solution that considers both interests.

The topic of jurisdiction has been discussed in chapter 2, and the first research question relates strongly to this chapter. The Internet and cyberspace have developed an orientation towards a different understanding of jurisdiction due to the omnipresent nature of the Internet. Territorial jurisdiction is not seen as a proper model of jurisdictional competence that could be applied to the Internet as it is. There exist different approaches to how Internet jurisdiction could be arranged instead of territorial model: country code Top Level Domains, end-to-end principle, service providers, or through the layers of Internet architecture, for example.

While moving forward from the Internet to cyberspace, the jurisdictional ideologies seem to move forward as well: cyberspace could be treated as a separate place where its own and distinct regulation applies; or cyberspace could develop its own legal system based on self-regulation; or cyberspace could be recognized as fourth international common. This is argued based on the separateness from the physical world and the a-territorial nature of cyberspace. However, this viewpoint can be criticized since the role of traditional legal tools can be underestimated: transactions occurring in cyberspace are not more unexceptional to the conflict of law tools than other international transactions.

Besides the nature of cyberspace and the jurisdictional discussions in relation to it, the jurisdiction of transnational private actors has been relevant for this research as well. Commonly technological development may be so rapid that regulation cannot keep up with the changes occurring, which has caused private actors to begin to develop their own standards.

Possibly the most common form of a private party obtaining governance power are multinational corporations based on their economic power, but such an authority can absorb other forms as well, such as cyber-communities based on their social power, for example. It seems that the rising autonomy of private actors is challenging the traditional hierarchical structure of a state as the ruler. Even if the rule-making by private actors would not be regarded as law from the legal positivist view, the *de facto* effects in society are occurring and causing effects similar to positive law.

The jurisdiction of autonomous code-based communities has been a central element of chapter 2, which analyzes the jurisdiction of cyberspace and the code as law of cyberspace. Three representations of legal frameworks have been a central part of the analysis: Lex Informatica, Lex Cryptographia, and Code is Law. These seem to be highly based on the cyber libertarian thoughts of the independence of cyberspace, treatment of cyberspace as a separate place, and code as a regulator. Lex Informatica is reasoned with the analogy originating from Lex Mercatoria, and the general implication from this analogy is that privately constituted legal systems that are independent of a state can exist. Lex Cryptographia recognizes that law is not the only regulator, but social norms are as well since private online communities are subject to their invisible consensus protocols. Code is Law could possibly be illustrated as a form of implementation of Lex Informatica and Lex Cryptographia since it proposes that code should be the law in cyberspace, but it must be recognized that legal rules and technical rules are not the same things.

Technological determinism features quite strongly in the jurisdictional framework of the Internet and cyberspace. As its strongest expression, it seems to attack the state jurisdiction and declare the independence of cyberspace where code is law that could form the rules of cyberspace. The problem with technological determinism is that it seems quite strongly to consider and endorse the positive side and outcomes of technology and does not comprehensively anticipate the negative ones, such as criminal activity, which has already been occurring with cryptocurrencies[300], for example.

Chapter 3 of the research focused on analyzing the current state of international blockchain regulation, and two approaches were recognized: either to develop new regulations or to adapt existing ones. Nevertheless, it must be recognized as well that these two approaches are still

[300] See Forbes 2021. Cryptocurrencies have been used for illicit financing and money laundering.

occurring at the same time and are not mutually exclusive. The principles of functional equivalence and technological neutrality were found as guiding principles for online law-making. Due to the practical limitation of research, two frameworks were chosen for analysis: Distributed Ledger Technology Regulatory Framework 2019 representing a new regulatory framework by ITU and UNCITRAL Model Laws representing the existing regulatory framework that is used for analyzing whether and how well existing laws could be adapted for blockchain technology. Regulation has a central role since it has a great impact on whether technological innovations will receive their full potential or if wrong and unfitted regulation will destroy the innovation. Regulatory uncertainty has been recognized as an obstacle for blockchain adoption, while some states have profiled themselves as blockchain hubs. In addition, a potential rise of blockchain havens is recognized as one possible negative outcome for the lack of regulation and effective policies.

The ITU framework is possibly the most comprehensive international legal framework for blockchain technology at the time of this research which is why it was chosen for the analysis. The framework is focusing on the regulatory issues, but the promise of practical recommendations for regulators could have been met better since partly it seems to be more focusing on recognizing the regulatory issues than providing some kind of solutions to them. Additionally, some of the recommendations were only brief listings, and one classification of the property lacked the recommendations completely. The framework is an example of developing new regulation for blockchain technology that can comprehensively take the special features of the technology into consideration. The role of private actors in blockchain is recognized, and the possibility that traditional regulatory approaches may not work for blockchain technology. However, the approach is more co-operative between balancing the private and public than promoting public control over blockchain technology. Yet, this approach does not promote technological determinism as its harder expression, but it could possibly represent softer technological determinism where it is understood that technology can influence human interactions and change human thoughts and understandings, which is why integrated solutions with existing legal systems are seen as the future rather than focusing the confrontations with governments and their control.

UNCITRAL Model Laws are an example of existing regulations that could be adapted to blockchain technology, and the focus of the analysis was if and how they could be adapted to blockchain technology. UNCITRAL Model Laws could provide clarity to smart contracts and

their validity and to the treatment of cryptocurrencies. However, UNCITRAL Model Laws do not seem to provide comprehensive opinions or thoughts to jurisdictional or governance issues but rather focuses more on specific blockchain applications or more specific details such as cryptocurrencies, smart contracts, securities, and registries, for example. Yet, UNCITRAL Model Laws are a more practical approach than the ITU framework. From the perspective of technological determinism, UNCITRAL Model Laws seem to focus more on the traditional public governance and law-making and do not view technology itself as such a strong influencer in society. Nevertheless, it must be noted that most of the UNCITRAL Model Laws were passed before the blockchain technology was even discovered. Overall, the current practice seems to be lacking concrete international level frameworks and approaches with actual legal acts fit for blockchain technology.

Chapter 4 of the research has focused on the topic of regulatory governance with *de lege ferenda* approach. As discovered in previous chapters of this research, blockchain technology involves a form of private rule-making in different forms: it is influencing human behavior and establishing blockchain communities, and guiding their behavior. Additionally, techno-libertarians have even proposed that cyberspace should form its own legal system based on self-regulation, which is quite a strong manifestation of technological determinism. Public international law is in a situation where rule-making has begun to develop on a private level creating similar effects to positive law. Possibly the goal is not how to bring these private actors and private law-making under public regulation and governance, but how to develop a regulatory governance system where both interests, public and private, can be taken into consideration and where they can co-exist in order to establish a proper functioning governance system. The confrontation between public and private may not be optimal in a globalized world.

International regulatory co-operation could function as a policy tool for establishing regulatory governance for blockchain technology since, among others, technological revolutions have interconnected the countries around the world. Globalization and an interconnected world have created changes to the global landscape that requires co-operation. One recognized challenge with international regulation is that non-legally binding instruments are more frequently used than legally binding ones, which leave more discretion on the national level. In order to receive better harmonization internationally, more binding actions would be needed. However, regulatory harmonization may not be the most optimal solution for blockchain technology at least its most substantive form since it may be practically hard to receive and blockchain

technology seems to represent a form of social technology to which the traditional governance models may not be sufficient solutions. Yet, there exists a contradiction between the powers of international organizations and the legal effect needed since international organizations are highly dependent on the member states and their willingness to co-operate.

A governance model for blockchain regulation in the future could be transnational governance or metagovernance, where public and private parties collaborate. Blockchain technology has specific governance elements based on the protocol rules written in the code and the human decision-making process of how the information is received. Additionally, networks such as blockchain have ultimately challenged the capability of traditional governance models to even govern networks, and the term governance has met redefinitions fit for network purposes.

The purpose of this research was to examine how technological determinism features in international blockchain regulation. Technological determinism features most significantly in the theoretical jurisdictional frameworks, and especially in Lex Mercatoria, Lex Cryptographia, and Code is Law which could even be illustrated as a form of an attack against the law. Technological development is viewed as the changing force in society so far that cyberspace should form its own legal system: technological development occurs to which society must absorb. Some softer form of technological determinism is observed with new law-making in which the specifics of blockchain technology have been taken into consideration. The role of transnational private actors has increased, which is challenging the role of law as understood in legal positivism since these private actors are able to establish rules and affect human behavior similar to positive law. However, it must be noted that technology is not the only determinant of the social change that is occurring, which is a much larger phenomenon overall and not driven by technological change solely. In this research, it is noted that technological determinism endorses the positive outcomes of technology and its development and does not quite consider the negative ones. Additionally, participating in blockchains is voluntary, and they are human creations; technology is not forcing itself on the members of society.

In addition to features of technological determinism, the purpose of this research was to examine the international jurisdictional challenges in relation to blockchain regulation and international regulatory governance fit for blockchain technology. Blockchain technology seems to create confuses over jurisdiction and applicable law, which has been noted in the literature. The omnipresent nature of cyberspace and the Internet have established a movement towards the idea of separate cyberspace jurisdiction where its own laws should apply.

Nevertheless, multijurisdictional issues have occurred before with international trade, for example, and the tools of international law exist to solve these jurisdictional challenges: cyberspace, and blockchain technology, is not such an exception that could not be solved with existing legal tools. The ideas of cyberspace as a separate place seem to represent more cyber-libertarian thoughts than the reality where technologies have been regulated in formal and informal ways through history.

Traditional government-centered or other central authority-based governance systems may not offer the best regulatory governance solutions for blockchain technology. The role of transnational private actors on international planes has increased and their ability to produce *de facto* rules. Blockchain technology is based on network communication, and the system represents a form of a counteraction to central authorities. The role of private actors is relevant, and instead of trying to pursue these private actors forcibly under public control, the objective towards more transnational governance where public and private parties collaborate could function more effectively. Nevertheless, it must be taken into consideration that technological change has occurred before, and blockchain technology may not itself represent something such a novel in nature that completely new regulatory governance systems should be developed just due to blockchain. As noted, globalization is already quite a vast phenomenon that has caused changes to public governance, and it may not be quite straightforward to establish the role of blockchain technology in this change, or could it be occurring without blockchain?

Another interesting viewpoint is that the future of blockchain technology is still quite uncertain and whether it will actually fundamentally change societies at large is unknown. There is a possibility that blockchain technology will never reach the predicted, cyber-libertarian, full potential. Does blockchain technology actually offer something groundbreaking, or is it just a distributed database that has been able to maintain the techno-hype without actually proving its value?