1. *Blockchain and Public Law: An introduction*

Oreste Pollicino and Giovanni De Gregorio

1. THE DOUBLE FACE OF BLOCKCHAIN TECHNOLOGIES

The development of digital technologies is influencing contemporary society leading to the rise of new languages, behaviours, lifestyles, organisations, and methods of industrial production. Digitisation offers a series of opportunities impacting on areas considered almost irreversible, opening new possibilities for the economy and radically reshaping traditional legal categories. The internet has already shown its role of disruptive technology producing significant breakdowns. The evolution of blockchain technologies will likely amplify this trend increasing the level of decentralisation to which the internet has already paved the way.¹

Blockchain applications are based on decentralised and distributed ledgers which can be used for various purposes, for instance, to exchange value or store information on public registries.² The distributed nature of the ledger means that it is maintained simultaneously across a network of unrelated computers or servers (i.e. nodes). Consequently, the ledger contains a regular and complete record of all transactions grouped into blocks: a block is only added to the chain if the nodes, which are members in the blockchain network with high levels of computing power, reach consensus on the next valid block to be added to the chain. In order to determine the validity of a block, miner nodes compete to solve a highly complex algorithm to verify it.

Once information is entered on the blockchain, it is extremely difficult to alter. A blockchain network usually lacks a centralised point of vulnerability and each block includes the previous block's hash. A blockchain network may be public and open (i.e. permissionless) like the internet but it can also be structured within a private group like an intranet (i.e. permissioned). As a result, it is possible to define blockchain as a distributed, shared, encrypted technology constituting an irreversible and incorruptible repository of information.

The expression 'blockchain' has acquired a metaphorical meaning.³ This word has become a synonym of digital revolution like the 'cyberspace' at the end of the last century.⁴ The

¹ Melania Swan, *Blockchain: Blueprint of a New Economy* (O'Reilly 2015).

² Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press 2018).

³ Melanie Swan and Primavera De Filippi, 'Towards a Philosophy of Blockchain' (2017) 48(5) *Metaphilosophy* 603.

⁴ According to Gibson:

After this first attempt, the cyberspace became prominently identified with online computer networks. Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts [...] A graphic rep-

primary characteristics of blockchain consisting of a resilient, decentralised, peer-to-peer network are the primary reasons for this belief. Cyberpunks considered peer-to-peer networks and encryption as instruments to foster personal freedom and liberty.⁵ Cryptography ensures individuals can exclude public and private actors from interfering with their freedoms.⁶ Individuals would emancipate themselves from public powers and companies' social control by virtue of the anonymity ensured by the use of cryptography. In this way, individuals could evade State prosecution and private harassment. In other words, cryptography is an instrument to protect individuals' privacy and political freedom.

The promise of blockchain, and, in general, distributed ledger technologies, is represented by the elimination of the middleman and the rise of the rule of the crowd.⁷ The elimination of entities which, at central level, validate certain transactions, exchanges, registers and their replacement with a consensus mechanism based on cryptography allows all participants in the distributed register to be able to trust the legitimacy of a given transaction without the necessity that the same is in some way validated by a central subject governed by public law. In this way, blockchain can be considered instruments to promote trust. Blockchain technologies enable, for the first time, unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority. For instance, automating transactions based on the immutable rules established by code would improve the efficiencies and transparency of public services and decrease tensions in private relationships.⁸

Nonetheless, these advantages also constitute the primary weakness that triggers fundamental legal questions.⁹ This revolution of freedom would face the drawback coming from the rise of a system of private governance escaping democratic oversight. Blockchain technologies minimise the role of the middleman facilitating the creation of autonomous systems on a more peer-to-peer basis. This process does not concern just traditional intermediaries like financial institutions but also the role of public authorities in enforcing policies in the blockchain environment. In this way, blockchain technologies would promote the development of autonomous systems providing a parallel model of governance competing with public authority, thus, building new private regulatory frameworks.¹⁰ Similarly to what Reidenberg called Lex

resentation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.

William Gibson, *Neuromancer* (Ace Books 1984), 67.

⁵ Donald Davis, 'A Brief History of Cryptography' (1997) 2(2) *Information Security Technical Report* 14.

⁶ David Chaum, 'Security Without Identification: Transaction Systems to Make Big Brother Obsolete' (1985) 28(10) *Communications of the ACM* 1030.

⁷ William Magnuson, *Blockchain Democracy: Technology, Law and the Rule of the Crowd* (Cambridge University Press 2020).

⁸ Helen Eenmaa and Maria José Schmidt-Kessen, 'Regulation Through Code as a Safeguard for Implementing Smart Contracts in No-Trust Environments' (2017) EUI Department of Law Research Paper No. 2017/13 <https://cadmus.eui.eu/handle/1814/47545> accessed 15 November 2020.

⁹ Aaron Wright and Primavera De Filippi, *Blockchain and the Law* (Harvard University Press 2018).

¹⁰ Michael Abramowicz, 'Cryptocurrency-Based Law' (2016) 58 *Arizona Law Review* 359.

Informatica,¹¹ here, as argued by Wright and De Filippi, it is possible to refer to the rise of Lex Cryptographia.¹² The role of ‘code as law’ can also be extended in the field of blockchain.¹³

This framework challenges the exercise of public powers and the rule of law.¹⁴ The trust in the blockchain environment would fall before the impossibility of public actors to enforce public policies and protect rights and freedoms. The characteristics of blockchain technologies raise questions about how constitutional democracies can regulate these technologies.¹⁵ The primary challenge consists of enforcing public policies to protect fundamental rights and democratic values against the exercise of unaccountable entities expressing their private sovereignty on the blockchain environment.

2. A NEW PHASE OF TECHNOLOGICAL LIBERTARIANISM?

The optimism around blockchain applications would represent a new phase of technological libertarianism. When looking at the crypto-anarchist manifesto by May,¹⁶ there are similarities with the debate about the regulation of the internet at the end of the last century. According to Narayanan, cryptoanarchism can be considered ‘a political philosophy that, in its idealized form, recognizes no laws except those that can be described by math and enforced by code’.¹⁷ Even the characteristics of the internet have led the first cyberspace scholars to consider the digital environment as being outside the scope of influence of public actors. Precisely, according to Barlow, cyberspace was a new world.¹⁸ The idea behind these two techno-libertarian movements was based primarily on the possibilities for individuals to enjoy their freedoms by virtue of anonymity and, more generally, the challenges governments address to enforce public policies in the digital environment. Put another way, Barlow and May expressed the same (liberal) promise: building an open society free from governmental or corporate interferences to rights and freedoms.¹⁹

¹¹ Joel R. Reidenberg, ‘Lex Informatica: The Formulation of Information Policy Rules through Technology’ (1997–1998) 76 *Texas Law Review* 553.

¹² Aaron Wright and Primavera De Filippi, ‘Decentralized Blockchain Technology and the Rise of Lex Cryptographia’ (2015) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 accessed 5 October 2020.

¹³ Karen Yeung, ‘Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law’ (2019) 82(2) *Modern Law Review* 207.

¹⁴ Thibault Schrepel, ‘Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia’ in Ulf Bernitz and others, *General Principles of EU Law and the EU Digital Order* (Wolter Kluwer 2020).

¹⁵ Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018); Kevin Werbach, ‘Trust, But Verify: Why the Blockchain Needs the Law’ (2018) 33 *Berkeley Technology Law Journal* 489.

¹⁶ Timothy May, ‘The Crypto Anarchist Manifesto’ (1992) <https://www.activism.net/cypherpunk/crypto-anarchy.html> accessed 15 October 2018.

¹⁷ Arvind Narayanan, ‘What Happened to the Crypto Dream?, Part 1’ (2013) 11(2) *IEEE Security & Privacy* 75.

¹⁸ John P. Barlow, ‘A Declaration of Independence of the Cyberspace’ (Electronic Frontier Foundation 1996) www.eff.org/cyberspace-independence accessed 16 June 2020.

¹⁹ Timothy May, ‘Crypto Anarchy and Virtual Communities’ (1994) <http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html> accessed 15 October 2020.

According to Johnson and Post, the only effective approach in cyberspace would be based on free-market regulation: by allowing users to choose the rules they find appropriate, new institutions and self-regulatory instruments would emerge from the digital realm.²⁰ A decentralised law resulting from customary or collective private action would be the basis for creating a democratic set of rules applied to digital communities.²¹ This bottom-up codification would reflect the values of the community whose legitimacy is based on the consent of the digital majority. Put in another way, rather than relying on traditional public law-making power to set the rules of cyberspace, every single digital community should be capable of participating in the creation of the new rules of their digital world. The well-known debate about the extraterritorial extension of national jurisdiction as resulting from the case *Licra v. Yahoo France* has confirmed these challenges.²²

This techno-enthusiasm can be explained by focusing on decentralisation. According to Benkler: '[d]ecentralization describes conditions under which the actions of many agents cohere and are effective despite the fact that they do not rely on reducing the number of people whose will counts to direct effective action'.²³ This differs from 'centralization', which 'is a particular response to the problem of how to make the behavior of many individual agents cohere into an effective pattern or achieve an effective result'.²⁴ Decentralisation constitutes a challenge for the exercise of public authorities whose scope and direction are limited to a specific space (i.e. territory) and population (i.e. citizens).

The internet has already underlined how decentralisation can affect how constitutional democracies exercise powers online. Unlike the control over traditional channels of communication bound by scarce resources, the internet offers a quasi-unlimited space increasing the complexities in monitoring its boundaries and apparently decreasing the need to ensure media pluralism through regulations.²⁵ Besides, traditional channels of communication are located in a specific territory with a limited geographical reach. On the contrary, the cross-border nature of the internet limits the ability of public actors to address phenomena occurring outside their territory. As a result, public powers increasingly rely on online intermediaries to enforce public policies in the digital environment.²⁶ Likewise, these challenges would also apply to blockchain applications since networks are primarily based on the internet architecture. The combination of peer-to-peer networks, cryptography and digital signatures describes a system which is not only decentralised but also resistant to tamper and disintermediated.

²⁰ David R. Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1367.

²¹ David R. Johnson and David Post, 'And How Shall the Net be Governed?' in Brian Kahin and James Keller (eds), *Coordinating the Internet* (MIT Press 1997).

²² *Licra et UEJF v. Yahoo Inc and Yahoo France* T.G.I. Paris 22 May 2000. See Joel R. Reidenberg, 'Yahoo and democracy on the Internet' (2001/2002) 42 *Jurimetrics* 261. *Yahoo!, Inc. v La Ligue Contre Le Racisme* 169 F. Supp. 2d 1181 (N.D. Cal. 2001). Regarding the topic of internet jurisdiction, see Dan J. B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017); Uta Kohl, *Jurisdiction and the Internet* (Cambridge University Press 2007).

²³ Yochai Benkler, *The Wealth of Networks* 62 (Yale University Press 2006).

²⁴ *Ibid.*

²⁵ Robin Mansell, 'New Media Competition and Access: The Scarcity-Abundance Dialectic' (1999) 1(2) *New Media and Society* 155.

²⁶ Micheal D. Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 *Virginia Journal of Law & Technology* 1.

Nonetheless, the internet has not realised a libertarian dream. States have successfully imposed their sovereign powers over online activities within their territory.²⁷ In countries where forms of surveillance and control over information are diffused, like China and the Arabic States, the internet has been subject to public control and surveillance which have led even to the blocking of online services.²⁸ Besides, the libertarian dream has not only faded away in relation to public actors' interferences with individual rights and freedoms. Instead of creating a democratic society based on bottom-up regulation, decentralisation has contributed to establishing an oligopoly of private entities who control information and define standards on how users exchange not only products and services but also content and data.²⁹ Therefore, it would be better to refer to platform-based regulation of the internet rather than a community-based regulation.³⁰

Both cases would confirm the positions of those scholars criticising the libertarian approach.³¹ Precisely, according to Lessig, governments are not 'passive dots' since they can express their influence on the four modalities defining the regulation of the cyberspace: law; social rules; economics; and network architecture.³² The last of which, in particular, constitutes the most effective way to regulate the internet since the possibility to influence the network structure increases the power of regulators to set the rules of the game online.³³ Unlike the static vision of the pathetic dot, organisations belonging to different social subsystems can be considered 'active dots' since they contribute to define their own rules and express their regulatory powers over other subsystems.³⁴ Notwithstanding all the actors contribute to shaping the overall picture, nodes have not the same influence on the network. Some dots in the network affect the structure of the cyberspace more than others. In other words, by virtue of their 'gravity', some actors in the network can attract other active dots shaping online communities and, as a result, the entire network.³⁵ These actors are usually called macro-nodes or gatekeepers.³⁶

Blockchain technologies do not eliminate any control. Only where the blockchain is permissionless, anyone can join the network and freely be involved in the process. For example, users can participate in block verification to create consensus or smart contracts such as, respectively,

²⁷ Barney Warf, 'Geographies of Global Internet Censorship' (2011) 76 *GeoJournal* 1.

²⁸ Ronal Delibert and others, *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT Press 2008); John G. Palfrey, 'Four Phases of Internet Regulation' (2010) 77(3) *Social Research* 981.

²⁹ Robin Mansell and Michele Javary, 'Emerging Internet Oligopolies: A Political Economy Analysis' in Arthur S. Miller and Warren J. Samuels (eds) *An Institutional Approach to Public Utilities Regulation* (Michigan State University Press 2002); Alex Moazed and Nicholas L. Johnson, *Modern Monopolies: What It Takes to Dominate the 21st Century Economy* (St. Martin's Press 2016).

³⁰ Orly Lobel, 'The Law of the Platforms' (2016) 101 *Minnesota Law Review* 87.

³¹ Jack Goldsmith, 'Against Cyberanarchy' (1998) 65 *The University of Chicago Law Review* 1199; Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006).

³² Lawrence Lessig, *Code 2.0: Code and Other Laws of Cyberspace* (Basic Books 2006).

³³ Francesca Musiani, 'Network Architecture as Internet Governance' (2013) 2(4) *Internet Policy Review* <https://policyreview.info/node/208/pdf> accessed 20 June 2018.

³⁴ Niklas Luhman, *Law as a Social System* (Oxford University Press 2008).

³⁵ Andrew Murray, 'Nodes and Gravity in Virtual Space' (2011) 5(2) *Legisprudence* 195.

³⁶ Emily B. Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers' (2012) 24(3) *International Review of Law, Computers & Technology* 263.

in the case of Bitcoin and Ethereum. In other cases, blockchain could be decentralised but permissioned. Some entities could impose the rules of the network on other users reintroducing the concept of the central authority. Unlike the case of public blockchains, only some actors can contribute to the consensus validating block transactions or creating smart contracts, thus, profoundly challenging the idea of disintermediation in the blockchain environment. Even in the case of permissionless blockchains, online intermediaries, full nodes and miners influence the functioning of the blockchain systems. These actors exercise regulatory influence over the blockchain environment. Looking at Bitcoin and Ethereum, in the last years, centralised pools of miners have emerged to share technical and human resources to increase the likelihood of rewards. As a result, four mining pools can exercise control over 50 per cent of the Bitcoin blockchain, and other three pools control 50 per cent of Ethereum.³⁷ Since these two systems are based on consensus, miners exercise regulatory influences on the entire network.

Turning back once again to the internet experience, according to Reed, the physical location of users was one of the primary reasons for the ‘cyberspace fallacy’.³⁸ Reed recognised that the weak point of libertarian positions depends on the physical substance of each individual which is located in a certain jurisdiction. Despite the complexities in ensuring the enforcement of the rules against primary infringers online, the idea behind this assumption underlined that cyberspace was not an area outside public power. Like in the case of the internet, the possibility to govern the blockchain environment highlights the ‘blockchain fallacy’ meaning that even distributed ledger technologies are subject to a mix of public power and private governance. Even if, at first glance, the peculiarities of blockchain technologies would realise the libertarian dream, however, going beyond this techno-enthusiastic narrative, it is possible to understand that blockchain technologies do not eliminate any regulatory power of public and private actors. Therefore, the question is not just about whether it is possible to regulate blockchain technologies, but also how constitutional democracies can deal with the rise of private determinations shaping fundamental rights and democracy in the blockchain environment.

While authoritarian regimes can exercise a broader control over blockchain applications by imposing extensive monitoring obligations on online intermediaries and shutting down the internet,³⁹ constitutional democracies cannot disproportionately interfere with the freedoms of the private sector or impose high surveillance and censorship obligations which would undermine individuals’ fundamental rights and freedoms. Since censorship and surveillance are exceptional measures for constitutional democracies, the primary challenge consists of understanding how public actors can express their regulatory powers over the entities operating in the blockchain environment. Therefore, the primary challenge for constitutional democracies would consist of limiting the influence of private ordering in the blockchain environment while protecting the principle of the rule of law and the possibility for citizens to participate in the governance of blockchain technologies through democratic circuits.

³⁷ See the hashrate of Bitcoin and Ethereum respectively on <https://blockchain.info/pools> and <https://etherscan.io/stat/miner?range=7&blocktype=blocks> accessed 14 November 2020.

³⁸ Chris Reed, *Internet Law: Text and Materials* 218 (Cambridge University Press 2007).

³⁹ Giovanni De Gregorio and Nicole Stremlau, ‘Internet Shutdowns and the Limits of the Law’ (2020) 14 *International Journal of Communication* 4224.

3. BLOCKCHAIN AND PUBLIC LAW: RESEARCH QUESTIONS

In the event blockchain technologies will really affect society as profoundly as it would promise,⁴⁰ it is worth assessing not only how these technologies challenge traditional categories of public law but also how constitutional democracies can exploit the potential of blockchain applications. These technologies can increase citizens' trust in public services.⁴¹ It is not by chance that different proposals include the implementation of blockchain technologies in the field of identification services,⁴² land registries,⁴³ and even to electronic voting.⁴⁴ Likewise, blockchain can also foster freedom of expression. In authoritarian regimes, these applications can limit the possibility for public actors to censor speech while allowing traditional media outlets to share information and news.⁴⁵ The implementation of cryptography can also foster the right to privacy, thus, promoting autonomy and self-determination.⁴⁶

Nonetheless, blockchain technologies can also marginalise public actors in areas of public interests such as health or financial markets as well as in relation to the enforcement of legal rules against illicit behaviours. These technologies could lead to a shift of power from legal rules adopted by public actors to a mix of private and technological rules established by decentralised and unaccountable entities. Blockchain does not raise novel tests for modern constitutionalism which is already exposed to the influence of global dynamics.⁴⁷ Precisely,

⁴⁰ Kelvin F. K. Low and Eliza Mik, 'Pause the Blockchain Legal Revolution' (2020) 69(1) *International and Comparative Law Quarterly* 135.

⁴¹ David Allessie, Maciej Sobolewski and Lorenzino Vaccari, 'Blockchain for Digital Government. An Assessment of Pioneering Implementations in Public Services' JRC Science for Policy Report (2019) https://publications.jrc.ec.europa.eu/repository/bitstream/JRC115049/blockchain_for_digital_government_online.pdf accessed 14 November 2020.

⁴² Andrej J. Zwitter, Oskar J. Gstrein and Evan Yap, 'Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual' *Frontiers in Blockchain* (28 May 2020) <https://www.frontiersin.org/articles/10.3389/fbloc.2020.00026/full> accessed 14 November 2020; Paul Dunphy and Fabien A. P. Petitcolas, 'A First Look at Identity Management Schemes on the Blockchain' (2018) 16(4) *IEEE Security and Privacy* 20.

⁴³ Maksymilian Ewendt, 'Leveraging Blockchain Technology in Property Records: Establishing Trust in a Risk-Filled Market' (2018) 19 *North Carolina Journal of Law & Technology* 99; Victoria L. Lemieux, 'Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective' (2017) 6(3) *European Property Law Journal* 392.

⁴⁴ Yoan Hermstrüwer, 'The Limits of Blockchain Democracy: A Transatlantic Perspective on Blockchain Voting Systems' (2020) TTLF Working Papers https://law.stanford.edu/wp-content/uploads/2020/01/hermstruewer_wp49.pdf accessed 4 November 2020; Desmond Johnson, 'Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values?' (2019) 10(2) *European Journal of Risk Regulation* 330; Mahtab Alam, Mukhtar Opeyemi Yusuf and Nazifi Alhassan Sani, 'Blockchain Technology for Electoral Process in Africa: A Short Review' (2020) 12 *International Journal of Information Technology* 861.

⁴⁵ Bernat Ivancsics, 'Blockchain in Journalism' *Columbia Journalism Review* (25 January 2019) https://www.cjr.org/tow_center_reports/blockchain-in-journalism.php accessed 12 November 2020.

⁴⁶ Jorge Bernal Bernabe and others, 'Privacy-Preserving Solutions for Blockchain: Review and Challenges' (2019) 7(1) *IEEE Access* 164908; Nir Kshetri, 'Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy' (2017) 41(10) *Telecommunications Policy* 1027.

⁴⁷ Eric C. Ip, 'Globalization and the Future of the Law of the Sovereign State' (2010) 8(3) *International Journal of Constitutional Law* 636; Mark Tushnet, 'The Inevitable Globalization of Constitutional Law' (2009) 49 *Virginia Journal of International Law* 985.

traditional boundaries of public law are challenged as private companies increase their regulatory influence over public actors by developing autonomous and decentralised technologies allowing them to run their business across borders.⁴⁸ Even if, at first glance, the marginalisation of public actors would foster rights and freedoms realising the dream of crypto-anarchic and cyberlibertarian theories, it also decreases the possibilities for public actors to protect individuals against the abuse of their fundamental rights by non-accountable actors.⁴⁹ Historically, liberal constitutionalism has been structured on a vertical dimension where the power to limit liberty is only the public one constrained by the national constitution which identifies a specific territory and population.⁵⁰ The challenges raised by blockchain technologies are likely to lead to a new phase of digital sovereignty where unaccountable entities increasingly exercise areas of powers in the information society. Likewise, the characteristics of blockchain technologies raise concerns for democratic values, precisely with regard to the ability of citizens to define the scope of their rights and freedoms within democratic circuits and oversight.

The ability of blockchain applications to cross jurisdictional boundaries raises concerns as the nodes on the network can be located anywhere in the world. This leads to wonder about not of complex jurisdictional issues but also the influences of States on such technologies.⁵¹ The lack of public enforcement in the blockchain environment could affect the protection of fundamental rights and freedoms. For instance, the incorruptibility of the blockchain can have serious implications for freedom of expression,⁵² as well as for privacy and data protection,⁵³ particularly when it is necessary to update or delete specific transactions including personal data. The transparency and incorruptibility of blockchain technologies are not easily compliant with the right to privacy, particularly in the European framework according to the General Data Protection Regulation.⁵⁴

Moreover, blockchain technologies challenge the role of public law also when looking at other legal fields. In the case of contract law, smart contracts are not only tools which are increasingly automating private agreements.⁵⁵ They are also self-executing contract contribute

⁴⁸ Oreste Pollicino and Marco Bassini, 'The Law of the Internet between Globalisation and Localization' in Miguel Maduro, Kaarlo Tuori and Suvi Sankari (eds), *Transnational Law. Rethinking European Law and Legal Thinking* (Cambridge University Press 2016).

⁴⁹ Gunther Teubner, 'Transnational Fundamental Rights: Horizontal Effect?' (2011) 40(3) *Netherlands Journal of Legal Philosophy* 191.

⁵⁰ Andras Sajó and Renata Uitz, *The Constitution of Freedom: An Introduction to Legal Constitutionalism* (Oxford University Press 2017).

⁵¹ Sarah Manski and Ben Manski, 'No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World' (2018) 29 *Law and Critique* 151.

⁵² Article 19, 'Blockchain and Freedom of Expression' (2019) <https://www.article19.org/wp-content/uploads/2019/07/Blockchain-and-FOE-v4.pdf> accessed 14 November 2020.

⁵³ Michèle Finck, 'Blockchains and Data Protection in the European Union' (2018) 1 *European Data Protection Law* 17; Christopher Kuner and others, 'Blockchain versus Data Protection' (2018) 8(2) *International Data Privacy Law* 103; Lokke Moerel, 'Blockchain & Data Protection ... and Why They Are Not on a Collision Course' (2018) 26(6) *European Review of Private Law* 825; Christopher Millard, 'Blockchain and Law: Incompatible Codes?' (2018) 34 *Computer Law and Security Review* 843.

⁵⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L 119/1.

⁵⁵ Giesela Rühl, 'Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts?' in Benedetta Cappelletto and Gherardo Carullo (eds), *Blockchain, Law and Governance* 159 (Springer

to disintermediating the role of public authorities, primarily judicial power. Likewise, new cryptocurrencies and financial assets have spread and provide new possibilities to exchange value on a global scale.⁵⁶ These new instruments raise challenges for public actors, precisely concerning the monopoly over printing money, the interest to ensure trust in the financial system and the tackle of financial crimes. Besides, blockchain technologies have also raised challenges for antitrust law.⁵⁷ This field plays a critical role in limiting the concentration of economic powers in the blockchain environment which could lead to the exercise of powers by unaccountable entities. These non-exhaustive considerations underline not only that the characteristics of blockchain technologies question other legal fields but also that these challenges affect public law.

These examples introduce the research questions of this book. This work aims at developing a comprehensive overview of the primary legal challenges brought by the rise of the blockchain in the field of public law, primarily with regard to the role of public actors in addressing the challenges and opportunities of these technologies. Assuming that this technology may be highly beneficial not only for economic and financial transactions but also for society, the project aims at coupling the analysis of this relationship with a deeper investigation of the impact of blockchain technologies on public law. The project tackles from the very beginning a key question, i.e., whether the new model of governance proposed by blockchain technologies based on the removal of middlemen and distributed trust, further than being beneficial from an economic perspective, may also be desirable from a legal standpoint. It is questioned whether this model brings about benefits that outweigh the importance attached to traditional players/middlemen. The grounding research questions of the book are the following: once agreed that blockchain is a ground-breaking technology, how traditional categories of public law such as sovereignty, citizenship and territory are shaped? What is the impact on funda-

2020); Nataliia Filatova, 'Smart Contracts from the Contract Law Perspective: Outlining New Regulatory Strategies' (2020) 28(3) *International Journal of Law and Information Technology* 217; Larry A. DiMatteo, Michel Cannarsa and Cristina Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019); Daniel Kraus, Thierry Obrist, Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Edward Elgar Publishing 2019); Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996) 16 *Extropy: Journal of Transhumanist Thought* 1 https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html accessed 14 November 2020.

⁵⁶ Daniel T. Stabile, Kimberly A. Prior and Andrew M. Hinkes, *Digital Assets and Blockchain Technology: U.S. Law and Regulation* (Edward Elgar Publishing 2020); Chris Brummer (ed.), *Cryptoassets: Legal, Regulatory, and Monetary Perspectives* (Oxford University Press 2019); Christian Rueckert, 'Cryptocurrencies and Fundamental Rights' (2019) 5(1) *Journal of Cybersecurity* 1; Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80(6) *Modern Law Review* 1073; Andres Guadamuz and Chris Marsden, 'Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies' (2015) 20(12) *First Monday* <https://firstmonday.org/ojs/index.php/fm/article/download/6198/5163> accessed 14 November 2020.

⁵⁷ Thibault Schrepel, 'Libra: A Concentrate of "Blockchain Antitrust"' (2020) 118 *Michigan Law Review Online* 160; Thibault Schrepel, 'Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox' (2019) 3 *Georgetown Law & Technology Review* 281; Ioannis Lianos, 'Blockchain Competition: Gaining Competitive Advantages in the Digital Economy: Competition Law Implications' in Philipp Hacker and others (eds), *Regulating Blockchain Techno-Social and Legal Challenges* (Oxford University Press 2019).

mental rights and democratic values? What are the policy options and institutional frameworks and values to adopt by lawmakers and regulatory authorities to ensure a fair balance between private interests such as competition and innovation and democracy?

4. THE STRUCTURE OF THE BOOK

The book is articulated in two sections. The first part examines how blockchain technologies affect traditional categories of public law. The second part highlights the challenges for public law deriving from the intersection between blockchain and other legal fields like contract law, financial law and antitrust law. This book does not only map the issues at stake like fundamental rights, citizenship, democracy and the role of public administration, but also provides a broader point of reference to understand the relationship between blockchain and the law.

In the first part, the issues relating to blockchain are addressed from different constitutional angles. The first chapters address some of the pillars of the post-Westphalian state, precisely, sovereignty, territory and citizenship. In Chapter 2, Kohl describes the blockchain utopia, thus, dismantling the rhetoric characterising deterritorialisation. Technological determinism and optimism would fail to show the reality of the blockchain environment. This chapter just opens the door to Chapter 3 on the relationship between blockchain and sovereignty. De Caria examines the challenges which states' sovereignty addresses in the age of decentralisation and to what extent states can exercise their powers over blockchain technologies. Chapter 4 enriches this analysis showing the relevance of blockchain technologies for citizenship. Gstrein and Kochenov underline how distributed ledger technologies can be an effective tool for resource distribution among citizens. Nonetheless, they question whether blockchain applications in the area of identity management will ultimately increase human dignity, or further manifest traditional patterns of discrimination and inequality.

The following chapters focus on how blockchain technologies could foster or hinder democratic values and examine the role of public administrations in the blockchain environment. In Chapter 5, Goossens analyses whether blockchain as a distributed ledger technology and smart contracts as rule-based algorithms could contribute to safeguarding important public values of democracy and the rule of law. Chapter 6 complements this analysis by looking at how it would be possible to face the challenges related to the rise of authoritarian models of governance. Precisely, Bell underlines that, although blockchain technologies make traditional authoritarianism less likely, they make a new kind of authoritarianism, born of decentralised autonomous organisations (DAOs). Another critical piece of the puzzle is the role of public administration. In Chapter 7, Hermstrüwer discusses the virtues and the limitations of blockchain technology in the context of public administration. The characteristics of blockchain like immutability could clash with institutional safeguards and procedures which are designed to ensure the principle of the rule of law.

Three further chapters of the first part examine the impact of blockchain technologies on fundamental rights and freedoms. Precisely, these chapters focus on freedom of expression, privacy, data protection and health. Chapter 8 underlines the impact of blockchain technologies on freedom of expression. De Gregorio underlines how the characteristics of these technologies can foster freedom of expression allowing, for instance, media outlets to escape from public censorship. At the same time, blockchain technologies have been used not only to transfer values but also to upload illegal online content. To deal with the spread of illicit

conducts online, this chapter underlines how States could rely on online intermediaries even if the legal regime of these entities based on the system of notice and takedown does not exactly fit with the peculiarities of the blockchain environment. Chapter 9 examines the challenges for privacy and data protection with a focus on the GDPR. In this case, De Hert and Kumar focus on the threats relating to the implementation of blockchain technologies in data-driven business. Few of blockchain characteristics are best suited with some data processing principles, but few are detrimental to the data subject and the enforcer at the same time. In Chapter 10, Motsi-Omoijiade and Kharlamov provide an overview of how distributed ledger technologies are currently being developed and deployed in the healthcare sector. They underline how these instruments are relevant for health and the limits of these technologies in the healthcare sector.

Besides, this book explores the legal challenges triggered by blockchain technologies focusing not only on categories of public law such as democracy, citizenship and fundamental rights. The second part of the book examines how even the relationship between blockchain technologies and other fields of law is relevant to capture relevant challenges for public law. Three chapters examine the relationship between blockchain and public law at the intersection with other legal fields. Chapter 11 addresses the topic of smart contracts. Sirena and Patti underline how blockchain technologies could lead to the automation of private relationships. Smart contracts may produce an excess of privatisation through innovative self-help mechanisms and the application of dispute resolution systems, thus, reducing the role of public powers in this field. Chapter 12 addresses the field of FinTech and crypto-assets. Annunziata examines how public actors are dealing with new financial instruments and currency competing with public monopoly and ensuring trust in the financial sector. In Chapter 13, the relationship between blockchain and public law is seen under the lens of antitrust. Maggiolino and Zoboli provide an antitrust-based roadmap to be applied to the blockchain environment, underlining how antitrust law does not require reforms to address blockchain technologies. Even if there are issues concerning the detectability of anti-competitive conducts and the opportunity to discuss the power of the authorities to effectively monitor the conduct of companies operating through blockchains, antitrust law could be a remedy against the exercise of decentralised powers.