Border Problems: Mapping the Third Border

Jason Grant Allen and Rosa María Lastra*

Abstract

In the last 20 years, the Internet has become the site of economically and legally relevant objects, events and actions. More recently, there has been a flurry of innovation in the financial application of this technology. 'Cyberspace' has therefore become the source of potential risks to the financial system. This article builds on one of the authors' prior work on 'border problems' in financial regulation, namely the border between the regulated and the unregulated and the border between national jurisdictions. This provides an entry point into a conceptual exploration of a third border between the 'real world' and 'cyberspace'—a domain of human interaction that is facilitated and conditioned by digital communications systems. Accepting the spatial metaphor *arguendo*, we offer some observations on the nature of both the 'real world' and cyberspace, with an eye towards locating, raising and guarding the boundary. We track the evolution of the 'cyber-sovereignty' debate and survey the divergent approaches currently taken to borders in cyberspace and their correlation to the broader geopolitical map of the early 21st century. Based on our understanding of financial stability and systemic risk, we argue that sovereign states still have a unique and irreplaceable role that must be reflected in the emerging law of Internet jurisdiction. We conclude with a few observations on how this could affect the design of financial regulation in the coming decade.

INTRODUCTION

Following the Global Financial Crisis ('GFC'), Goodhart and Lastra presented a 'border problems' metaphor to highlight two basic tensions in the regulation of financial markets. Their

* Dr Jason Grant Allen is a Senior Fellow at the Weizenbaum Institute for the Networked Society. He also holds affiliations at the Humboldt University of Berlin Centre for British Studies, UNSW Faculty of Law, University of Tasmania Faculty of Law, and the Cambridge Centre for Alternative Finance. Professor Rosa María Lastra is the Sir John Lubbock Chair in Banking Law at the Centre for Commercial Law Studies, Queen Mary University of London (QMUL).

This article was presented at the Sheffield Institute for Corporate and Commercial Law 4th Law and Money Conference, *Banking in the Shadows – FinTech, Cryptocurrencies and Emerging Financial Systems* (University of Sheffield, 3 September 2018), at the International Workshop on Financial System Architecture and Stability 2018 (Cass Business School, 10-11 September 2018), at the LSE Systemic Risk Centre conference, *The Future of Money and the Impact of Fintech and Cryptocurrencies* (LSE London, 26 November 2018), and it served as the Background Paper for the *4th CCLS-Bank of England Conference* (Bank of England, 4 July 2019). The authors would like to thank the organisers and participants of these events for their valuable feedback. The authors would also like to thank Professor Ross Buckley, Dr Anton Didenko, Professor Campbell McLachlan, Professor Chris Reed, and Dr Jörg Pohle for their comments, as well as the anonymous reviewers. The usual disclaimer applies. J.G. Allen gratefully acknowledges the financial support of the Alexander von Humboldt Foundation. All URLs last accessed 17 September 2019.

metaphor comprised two borders: the first border between regulated and unregulated activities and entities, and the second border between national jurisdictions.[1] When these borders are crossed (whether by a regulated entity engaging in unregulated activities, an unregulated entity engaging in regulated activities, or a foreign entity engaging in regulated activities in the jurisdiction, an economy faces risks originating in unregulated spaces, with potential implications for both consumer protection and financial stability.

Since the 1990s, the Internet has become integral to many economically important—and therefore *prima facie* legally relevant—objects, events and actions.[2] Modern information and communications technology ('ICT') makes transacting across geographical distance quicker, easier, more secure, and less expensive, reducing many of the hurdles faced previously to trading with counter-parties based in different places. Currently, innovations in financial technology ('Fintech') are making the Internet an important channel for the delivery of financial services and products.[3] Fintech-driven financial services are diverse, including finance and investment (eg, crowdfunding and peer-to-peer lending), payments, money, exchanges and infrastructure (eg, mobile money, virtual currencies including 'cryptocurrencies', and foreign exchange), and consumer interface (eg mobile application-based financial services).[4] Many of these operate in the 'shadow' industry, ie in parallel to conventional, regulated firms. Although Fintech-based financial products and services are subject to existing regulations, and although existing regulations are capable of applying to novel socio-technological practices, the growth of Fintech could cause 'border problems' because it (i) delivers new financial products and services that have not yet been regulated (eg 'cryptoassets'[5]), (ii) utilizes new forms of business organisation that are not necessarily recognized by the legal system (eg, 'distributed autonomous organisations'), and (iii) operates in a 'space' which is, by nature, non-territorial or difficult to define in terms of territorial jurisdiction.[6]

The notion of 'cyberspace' itself helps to understand the potential risks posed by Internet-based financial services. As the term implies, cyberspace is the communications within a network of digital computers *conceptualised as a place*. In a seminal (if now dated) article,[7] Johnson and

[1] C.A.E. Goodhart and R.M. Lastra, 'Border Problems' (2010) 13(3) *Journal of International Economic Law* 705.

[2] See P. Brey, 'The Social Ontology of Virtual Environments' (2003) 62(1) *American Journal of Economics and Sociology* 269, 269.

[3] See D.W. Arner, J.N. Barberis, and R.P. Buckley, 'FinTech and RegTech in a Nutshell, and the Future in a Sandbox' (2017) 3(4) *CFA Institute Research Foundation Briefs* 1; D.W. Arner, J.N. Barberis, and R.P. Buckley, 'FinTech, RegTech, and the Reconceptualization of Financial Regulation' (2017) 37 *Northwestern Journal of Law & Business* 371.

[4] See D.W. Arner, J.N. Barberis, and R.P. Buckley, 'The Evolution of FinTech: A New Post-Crisis Paradigm?' (2015) 47 *Georgetown Journal of International Law* 1271.

[5] See A. Blandin, A.S. Cloots, H. Hussain, M. Rauchs, R. Saleuddin, J.G. Allen, K. Cloud, and B. Zhang, 'Global Cryptoasset Regulatory Landscape Study' (Cambridge Centre for Alternative Finance, 16 April 2019), URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379219.

[6] See C. Reed, 'Taking Sides on Technology Neutrality' (2007) 4(3) *SCRIPT-ed* 263.

[7] For a critical appraisal, see eg, D. Hunter, 'Cyberspace as Place and the Tragedy of the Digital Anticommons' (2003) 91(2) *California Law Review* 439; M.A. Lemley, 'Place and Cyberspace' (2003) 91(2) *California Law*

Post argued that global computer-based communications systems cut across territorial borders, 'creating a new realm of human activity and undermining the feasibility […] of laws based on geographic boundaries.'[8] This new 'realm' of human activity exists in something analogous to physical space:

> While these electronic communications play havoc with geographic boundaries, a new boundary, made up of screens and passwords that separate the virtual from the 'real world' of atoms, emerges. This new boundary defines a distinct Cyberspace.[9]

The stronger claims of the 'cyber-sovereignty' literature of the 1990s have not been accepted in the mainstream scholarship[10] while the advent of distributed ledger technology ('DLT') has added a new layer of complexity to the landscape.[11] But the metaphor of place-ness has stuck, and it is on this notion that we wish to focus. We incorporate the notion of cyberspace into the 'border problems' model by adding a *third border* between the 'real world' and 'cyperspace' (terms we define below), jand examine the impact of Fintech on conventional financial regulation.

The objective of financial stability has become mainstream in the decade since the GFC, but it has yet to be sufficiently anchored in a legal and jurisprudential basis. Financial stability remains a broad and discretionary concept and the economics and legal professions have not reached a commonly agreed definition, even though there is consensus about its relation to the prevention and containment of systemic risk. Given the transnational nature of systemic risk generally, the pursuit of financial stability interacts awkwardly with the notion of national territorial jurisdiction—especially in the context of cyberspace.

Bearing in mind this financial stability objective, the main contribution of this article is the development of a conceptual framework for the regulation of Internet-based financial services. We draw on an interdisciplinary approach that combines financial law, regulatory theory, social ontology, and, more peripherally, transnational legal theory and critical studies of legal geography. The framework that emerges also provides an inroad into the broader 'Internet jurisdiction' debate.

The article, which integrates the third border in financial regulation with the complexities of cyberspace jurisdiction, is divided into six sections following this introduction. First, we provide some context by discussing the nature of 'financial cartography', or the landscape that our borders are imposed upon. This section is important because it explains what the three

---

Review 521. Hunter provides a detailed history of the first decade of the early years of 'cyberspace as a place' and we will not repeat that here.

[8] D.R. Johnson and D.G. Post, 'Law and Borders—The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1367.

[9] *ibid*.

[10] See C. Reed, *Making Laws for Cyberspace* (Oxford 2012), 7, citing *inter alia* J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford 2006), 142.

[11] See generally Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018).

borders borders are and why they are important. We then elaborate on what we have identified as the two 'known borders', highlighting the relevant features that we think will help us to understand the posited third border. In particular, we explain what we understand by 'regulated activities', 'regulated entities', and 'territorial jurisdiction'. We then introduce our third border and, in order to do so, set out a conception of 'cyberspace'. The penultimate section explores how the border between 'cyberspace' and the 'real world' operates in the important context of financial services, and how it might be guarded against systemic risk. We conclude with some recommendations and questions for further research.

SOME OBSERVATIONS ON FINANCIAL CARTOGRAPHY

Before mapping our borders, it is convenient to consider the 'topography' that they transect. Fundamentally, the borders are under constant pressure because applicable regulation penalises those within the regulated space, relative to those outside it, causing substitution flows towards the unregulated space. According to Goodhart and Lastra:

> If regulation is effective, it will constrain [those engaging in regulated activities] from achieving their preferred, unrestricted position, often by lowering their profitability and their return on capital. So the returns achievable in the regulated sector are likely to fall relative to those available on substitutes outside of it. There will be a switch of business from the regulated to the unregulated. In order to protect their own business, those in the regulated sector will seek to open up connected operations in the non-regulated sector to enable them to catch the better opportunities there.[12]

The topography of markets is such that, like water, financial activity flows downhill and around high points. For example, commercial banks opened up associated conduits, structured investment vehicles, and hedge funds, which contributed to the GFC. This pressure has perhaps increased with the enhanced burden of compliance following the GFC, and the means of border crossing have potentially increased. Like territorial waters in international maritime law, borders are often the source of conflicts.

As an example of the pressure behind substitution flows, our recent analysis pointed to so-called 'virtual currencies' as a new frontier of financial activity: 'virtual currency' schemes may constitute 'grey' currency issues, securities issues, and payment rails, for example, operating in parallel to regulated financial services. [13] The sale of equity-like tokens in Initial Coin Offerings ('ICOs') as a substitute for conventional debt or equity securities saw a massive flow of capital into early stage ventures in 2017, many of which effectively circumvented

---

[12] Goodhart and Lastra, n 1 above, 706. See also C.A.E. Goodhart, 'The Boundary Problem in Financial Regulation' (2008) 206 *National Institute Economic Review* 48.

[13] R.M. Lastra and J.G. Allen, 'Virtual Currencies in the Eurosystem: challenges ahead' prepared for the Committee on Economic and Monetary Affairs of the European Parliament (ECON) as an input for the Monetary Dialogue of 9 July 2018 between ECON and the President of the European Central Bank (http://www.europarl.europa.eu/committees/en/econ/monetary-dialogue.html). Also published as R.M. Lastra and J.G. Allen, 'Virtual Currencies in the Eurosystem: Challenges Ahead' (2019) 52(2) *The International Lawyer* 177. See Libra Association, *An Introduction to Libra* (18 July 2019), URL: See https://libra.org/en-US/white-paper/?noredirect=en-US.

capital markets and consumer protection requirements such as prospectus disclosure and corporate governance (eg, listing) standards that would otherwise have applied. 'Cryptocurrency'-based financial services are also frequently concentrated in permissive jurisdictions, from where they aim to service consumers in more strictly regulated markets.[14] Although we concluded that the overall size of the 'crypto' market was probably not yet systemic, there are significant incentives for institutional money to flow into the new crypto-token based financial economy, and we recommended that regulators remain vigilant, and the recent Libra proposal has borne out our analysis.[15] Another example comes from the rise in peer-to-peer lending and other 'informal' financial arrangements in China. As Braggion, Manconi and Zhu explain, Fintech-based peer-to-peer lending such as that over the *RenrenDai* platform may have helped to circumvent loan-to-value mortgage caps in recent years.[16]

The relation between the borders

As our analysis unfolds, the second border will appear as an outgrowth of the first. Financial regulation (ultimately) takes place at a national level, but financial activity is transnational, so national financial systems are inherently vulnerable to the effect of actions taken outside the jurisdiction. Supra-national rules, such as those found in the European Union, are still supra-*national*—they are derived from the communication and agreement between nation states. Entities that are unregulated because they are *foreign* are a category of unregulated entities. Again, incentives exist for those providing financial products and services to base themselves in a less regulated jurisdiction and, from there, to access more regulated markets where they will enjoy a comparative advantage.

The third border is an aspect of the first, as well: Activities that take place in (apparently non-jurisdictional) cyberspace are just a sub-set of (nationally) unregulated activities. However, just as the national border adds some explanatory power to the metaphor, ie, by allowing us to isolate the relevant issues of national jurisdiction *versus* international financial transactions, the third border highlights the relevant issues conventional regulators face when attempting to govern objects, events and actions in cyberspace. Chief among these are: (i) bringing cyberspace into a normative framework based on territorial jurisdiction and (ii) governing financial objects, events, and actions that are enabled by novel ICT—what Arner, Barberis, and Buckley call 'FinTech 3.0'. FinTech 1.0, they argue, began with early telecommunications cables in the mid-19th century and ended with early digitalisation in the 1960s. FinTech 2.0 continued until the late 2000s and was characterised by systems like Bankers' Automated Clearing Services ('BACS'), Clearing House Information Systems ('CHIS'), and Society of

[14] For example, a Frankfurt-based Fintech called 'Savedroid' was recently reported to be planning savings plans based in another European country for consumers in the German market. See R. Berschens, 'EU erwägt striktere Regeln für Bitcoin & Co.' (*Handelsblatt*, 4 September 2018), https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/kryptowaehrungen-eu-erwaegt-striktere-regeln-fuer-bitcoin-und-co-/22993608.html?ticket=ST-10029229-YhugI233f6vyAUTE9CLk-ap2.

[15] Lastra and Allen, n 14 above.

[16] F. Braggion, A. Manconi and H. Zhu, 'Can Technology Undermine Macroprudential Regulation? Evidence from Peer-to-Peer Credit in China' (IWFSAS, Cass Business School, 10 September 2018). Available at SSRN: https://ssrn.com/abstract=2957411.

Worldwide Financial Communications ('SWIFT'). FinTech 3.0 is characterised by novel objects and modes of action (such as crypto-tokens, cloud-based computing, and DLT), by changed business models and players (not only start-ups but also technology and telecommunications companies entering into the financial services sector)[17] and by attempts to disintermediate and/or automate intermediation. This, in our view, raises challenges for conventional regulation which is still often based on physical documents, centralised actors (especially intermediaries), and centralised information repositories.

Mapping the third border is especially difficult, however, because it requires a plausible account of cyberspace as a domain in which legally cognisable objects exist, legally relevant events take place, and legal acts (acts-in-the-law as well as legally relevant acts such as torts) are performed. This, we argue, is not only inherently difficult, but it can also unsettle some intuitive understandings of the 'real world'. Developing such an account, however, positions us well to understand how the technological processes that mediate our social interactions inform the structure of our social world itself, including the law. Part of the effort required is to describe *legally* what Tom Boellstorff calls the 'digital real'.[18] The effort is worthwhile because, with such an understanding, we can respond more intelligently and proactively to new forms of financial activity in the coming decades.

THE KNOWN BORDERS

The two borders discussed by Goodhart and Lastra are familiar subject matter; lawyers are used to categorising the world of possible objects, events and actions as 'regulated' and 'unregulated', with reference to the first border, and, using the second border, to carving the world up into so many national 'jurisdictions' (ie, spheres in which legal rules apply or have force). In this Section, we discuss both of these 'known borders', beginning first with what we mean by 'regulated activity', 'regulated entity', and—because it is essential to understanding how law behaves spatially—by 'jurisdiction'.

Regulated activities and entities

The term 'regulated' is predicated of both *activities* and *entities*. The primary implication of something being a 'regulated activity' is one of modal logic; a regulated activity is one that is *permitted* subject to conditions—which is to say it is sometimes *prohibited*, and possibly sometimes *obligatory*, but neither prohibited nor obligatory in all cases. It is tautological that everything which is not prohibited is permitted. Generally, the default mode in a free market economic order is permissive rather than prohibitive. However, due to the potentially harmful nature of some activities, the default mode is sometimes prohibition. In such cases, a *positive*

[17] See Arner, Barberis and Buckley, above n 4, 1278 *et seq*. Much of the current banking system still relies on Fintech 1.0 infrastructure. As we explain below, there is some overlap between FinTech 2.0 and FinTech 3.0, as the later stages of the former utilised Internet-based ICT.

[18] See T. Boellstorff, 'For Whom the Ontology Turns: Theorizing the Digital Real' (2016) 57(4) *Current Anthropology* 387.

permission (eg, a 'licence') is required, which is generally granted to a certain entity on terms. Driving is an activity that is prohibited except for licensed drivers. Lending to consumers is another. This is usually what is meant by 'regulated activities' in the financial services context—to be more precise, '*prima facie* prohibited activity permissible with a license'. The terms 'licence', 'charter', 'authorisation' (associated with the 'entry into the business' of commercial banks, for example)[19] indicate an exercise of government authority that has a sovereign-like character, in contrast to registration procedures which can be characterized as market regulation mechanisms that give 'access to the business'.

What does it mean for an *entity*, then, as distinct from an activity, to be regulated? In usage, it is usually the 'positive permission' sense that is intended. Saying that an entity is regulated is more likely to imply that the activity in question is *prima facie* prohibited, that a positive permission (licence) is required, and that the entity has been licensed such that *it* is permitted to do what others may not. So a regulated entity is either one with a positive permission or the kind of entity that engages in activities that are 'regulated' in the sense of being subject to oversight.

What is less obvious when we say that an activity is regulated is the implicit proposition that the activity is *possible* in the first place (by the relevant entity). In his seminal work, Lawrence Lessig discusses the constraints and affordances of the 'architecture' of the relevant world.[20] There was no point in saying that flying was regulated until flight became a technological possibility in the 20th century; there was no point in saying that *unmanned* flight was regulated until drones became a possibility in the 21st century. ICT makes new forms of activity possible, too. This leads to a very important point: The law responds to developments, often technology-led, which expand the horizons of what is possible; once the space of the possible has expanded, the law has to determine whether the space of the permitted expands with it or remains more constrained. Whether constraint takes the form of the extension of an existing regulation or the creation of a new one is of secondary importance. The idea of technology neutral regulation, then, is regulation that is broad enough to cover outcomes enabled by new technology without the need for reform. In this, the challenge is always to determine whether technology allows new forms of action, or simply provides new ways of doing old things.

'Fintech' follows a deep pattern in the history of finance, namely of new technologies (eg the printing press, DLT) enabling new forms of market activity to which the law must respond dynamically. As Katharina Pistor argues, the world of finance is legally constructed in a

[19] In the UK, no person can carry on 'regulated activities' by way of business unless authorised or exempt (section 19, Financial Services and Markets Act, FSMA). The regulated activities are specified in the FSMA (Regulated Activities) Order 2001 (RAO). Any firm that wants to be a bank (carrying on the regulated activity of accepting deposits) must be authorised to do this by the Prudential Regulation Authority (PRA). In the euro area, the ECB is exclusively competent to authorise credit institutions according to Article 4.1(a) of the SSM Regulation (Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions). In the USA, national banks are chartered by the Office of the Comptroller of the Currency.

[20] See L. Lessig, *Code version 2.0* (Basic Books 2006); L. Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

'dynamic process in which the rules of the game are continuously challenged by new contractual devices, which in turn seek legal vindication.'[21] Increasingly, these 'contractual devices' rest on forms of action enabled by novel ICT. The significance of this appears when we come to explore cyberspace as a site of actions, including novel financial transactions, that are not possible in the physical world. Behaviour in online spaces can be controlled not just by the modality of law but by the constraints of architecture that makes certain forms of action possible or impossible. This observation both promises new forms of liberal regulation in digital environments and warns of new forms of authoritarian control. This is one further reason why the debate about Internet jurisdiction is so important.

Territorial jurisdiction

The second border embodies the concept of sovereignty, as anchored in territorial jurisdiction. Broadly stated, a *jurisdiction* is a context in which some set of rules applies, and generally in which some institution is authorised by those rules to enforce them. Although the term is ubiquitous, the concept of jurisdiction continues to bedevil theorists.[22]

Jurisdiction becomes important when parties transact across borders. The rule-set of Jurisdiction A may treat objects, events, and actions differently to the rule-set of Jurisdiction B, and by definition each jurisdiction has different institutions of authority to make, interpret, and apply its rules. The aspect on which we wish to focus in our paper is captured well by the German term *Geltungsbereich*—that is the area [*Bereich*] in which laws *gelten*, which means to be valid and in force.[23]

Some communities operate with a notion of *personal* jurisdiction.[24] There, the context in which a rule-set applies is derived by ancestry or religion or oath of allegiance. But, perhaps because human communities (traditionally) occupy physical space and (often) claim exclusive law-making power over that space, modern conceptions of jurisdiction have a *territorial* basis. Territorial jurisdictions are defined by reference to geographical coordinates, be they natural landmarks or man-made lines on the earth's surface. Jurisdiction also extends into the earth and into the air, but only to a certain extent—no country can realistically claim a wedge of the universe extending from its surface *ad infinitum* .[25] Systems of purely personal jurisdiction are rare; more common are spheres of personal jurisdiction under the aegis of a territorial sovereign, such as the status of Jews in the Holy Roman Empire or under the Ottoman *millet*

[21] K. Pistor, 'A Legal Theory of Finance' (2013) 41 *Journal of Comparative Economics* 315, 316.

[22] F.A. Mann's classical conception of jurisdiction in international law is one of the inherent power of a state to regulate conduct, such power comprising the authority to legislate and the authority to enforce. See F.A. Mann, 'The Doctrine of Jurisdiction in International Law' (1964) 111 *Recuil des Cours* 1.

[23] We lack a cognate in English: E. Bulygin, 'Valid Law and Law in Force' in E. Bulygin (C. Bernal *et al* eds.), *Essays in Legal Philosophy* (Oxford 2015), 285.

[24] For example, Malaysia applies *syariah* law to Muslims only under Article 121(1A) of the Constitution of Malaysia.

[25] On airspace sovereignty generally see A.I. Moon Jr., 'A Look at Airspace Sovereignty' (1963) 29 *Journal of Air Law & Commerce* 328.

system.[26] Extra-territorial and even universal jurisdiction is of course claimed by states in certain contexts, but rather as an exception than as a rule.[27] In our view, the *personal* extra-territorial jurisdiction claimed by states is a promising starting point from which to consider jurisdiction in cyberspace.

The paradigm example of territorial jurisdiction is the 'Westphalian sovereign state', a form of geo-political ordering in which one community claims to possess sole law-making power over a defined territory, which means that it is (i) superior to any other rule-generating organisation within the territory and (ii) independent of any rule-generating organ outside the territory but (iii) makes no claims (in the ordinary case) to generate valid rules outside the territory. Intuitively, when we think of jurisdiction today we tend to think of states—thereby taking territorial jurisdiction for granted. Sovereignty is defined as the supreme authority within a territory, and the state is defined as the set of political institutions in which sovereignty is embodied.[28]

Because of this, territorial jurisdictions appear intuitively as parts of the earth, parts of the 'real world' or, as Johnson and Post put it, the 'world of atoms'.[29] Of course, this is not the case; a territory is a set of *geographical coordinates* projected onto the world of atoms;[30] the state is no more a given feature of the natural world than a centimetre or a country club.[31] The artificial, even quasi-abstract nature of nation states thus forms a major theme in this article.[32]

The ontic furniture[33] of our world sometimes makes more sense if we start with less grandiose examples than the nation state. Let us take some examples of 'jurisdiction' writ small, such as

---

[26] See eg K. Barley and G. Gavrilis, 'The Ottoman Millet System: Non-Territorial Autonomy and its Contemporary Legacy' (2016) 15(1) *Ethnopolitics* 24; R. Gechtman, 'Jews and Non-Territorial Autonomy: Political Programmes and Historical Perspectives' (2016) 15(1) *Ethnopolitics* 66.

[27] See 'Singapore warns citizens against legal cannabis use overseas' (*New Straits Times*, 27 October 2018), https://www.nst.com.my/world/2018/10/425482/singapore-warns-citizens-against-legal-cannabis-use-overseas.

[28] For further discussion, see R.M. Lastra, *International Financial and Monetary Law* (Oxford University Press 2015), ch 1.

[29] Johnson and Post, above n 8, 1368

[30] See generally B. Smith, 'On Drawing Lines on a Map' in A.U. Frank, W. Kuhn and D.M. Mark (eds.), *Spatial Information Theory: Proceedings of COSIT '95* (Springer 1995).

[31] On the ontology of the state, see eg D. Tan, 'The Metaphysics of Statehood' (2018) 31(2) *Canadian Journal of Law & Jurisprudence* 403. See also Joseph Raz, 'Why the State' and D. von Daniels, 'A Genealogical Perspective on Pluralist Jurisprudence' in N. Roughan and A. Halpin (eds.), *In Pursuit of Pluralist Jurisprudence* (Cambridge 2017), ch 7 and ch 8 respectively. See also C. von Bar, *Gemeineuropäisches Sachenrecht* (C.H. Beck 2015), para [186] for a parallel discussion in the private law of property.

[32] See eg, E.H. Robinson, 'A Documentary Theory of States and Their Existence as Quasi-Abstract Entities' (2014) 19(3) *Geopolitics* 461. There is a significant critical literature on the artificial nature of borders. See eg, A. Kaushal, 'The Politics of Jurisdiction' (2015) 78(5) *Modern Law Review* 759; A. Shachar, *The Shifting Border: Legal Cartographies of Migration and Mobility* (forthcoming Manchester University Press 2020); S.D. McDowell, P.E. Steinberg, and T.K. Tomasello, *Managing the Infosphere: Governance, Technology, and Cultural Practice in Motion* (Temple University Press 2007); L. Volpp, 'Imaginings of Space in Immigration Law' (2012) *Law, Culture and the Humanities* 1.

[33] See U. Mäki, 'Scientific Realism as a Challenge to Economics (and Vice Versa)' (2011) 18(1) *Journal of Economic Methodology* 1, 8; see also U. Mäki, 'Scientific Realism and some Peculiarities of Economics' in R.S.

the *eruv*, which allows us to bracket out considerations of institutional competence and the external aspect of sovereignty and to focus on jurisdiction as a *legally-constituted social delimitation of physical space*. An *eruv* is an urban area demarcated within a larger urban area by means of a boundary, usually marked by given landmarks such as telephone poles, by some sort of wall or fence or by virtue of its topography.[34] The purpose of an *eruv* is to turn an area according to Jewish law into a 'private' domain, instead of a 'public' one, such that certain prohibitions (eg, of carrying objects outside the private domain on *Shabbat*) do not apply. An *eruv* is specific to the community that creates it; communities from the same city that follow different traditions may not regard each other's *eruv* as kosher. It is an invisible border, defined by reference to landmarks, that has important deontic consequences, specifically enlarging the scope of permissible actions for those that create it. Similarly, so-called *cippi* stones mark the *pomerium* of ancient Rome. This line was originally (probably) a defensive wall, but by classical times it had already come to assume symbolic function. The *pomerium* played an important role in the legal and religious life of the city, closely entangled as they were. To stay with a prohibition on carrying, citizens were not allowed to carry arms within the *pomerium*.[35]

These two geographically-defined social spaces differ in important respects, but both are community-specific,[36] and both are connected to the physical world in an essential, rather than a casual way, because they are intended to divide and mark the space in which a community lives. Moreover, both fall squarely within the social part of our world, not the world of atoms.[37] Territorial jurisdictions are themselves defined in legal terms; as Peer Zumbansen notes, spaces of legal norm-creation may be defined by geographical territory, but they are demarcated by boundaries that are inseparable from the association of that space with a particular institutional infrastructure.[38]

If jurisdiction is not just a straightforward division of physical space, might it not interact with non-spatial 'places' such as 'cyberspace'? Consonant with the borders metaphor, the following sections of this article explore cyberspace as a new kind of 'territory' in which legal notions of

---

Cohen, R. Hilpinen, and Q. Renzong (eds), *Realism and Anti-Realism in the Philosophy of Science* (Kluwer 1996).

[34] See B. Smith, 'On Place and Space: The Ontology of the Eruv' in C. Kanzian (ed.), *Cultures: Conflict—Analysis—Dialogue: Proceedings of the 29 International Ludwig Wittgenstein Symposium* (Ontos 2007), 403. See also M. Rapoport, 'Creating Place, Creating Community: The Intangible Boundaries of the Jewish "Eruv"' (2011) 29(5) *Environment and Planning D: Society and Space* 891; B. Smith and L. Zaibert, 'Real Estate: The Foundations of the Ontology of Property' in H. Stuckenschmidt, E. Stubkjaer, and C. Schlieder (eds.), *The Ontology and Modelling of Real Estate Transactions* (Ashgate 2003).

[35] See S.B. Platner (T. Ashby ed.), *A Topographical Dictionary of Ancient Rome* (Oxford University Press 1929), '*pomerium*'.

[36] On the type of intersubjective intentionality founding groups, see R. Tuomela, *Social Ontology: Collective Intentionality and Group Agents* (Oxford University Press 2013), 220.

[37] See D.G. Post, 'How the Internet is making jurisdiction sexy (again)' (2017) 25 *International Journal of Law and Information Technology* 249, 250; see broadly J. Searle, *Making the Social World* (Oxford University Press 2010), 3.

[38] P. Zambunsen, 'The Regulatory Landscape of Global Governance and Transnational Legal Authority' in G. Handl, J. Zekoll and P. Zumbansen (eds.), *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (Brill 2012), 551.

jurisdiction might operate, or at least interact. As Mariana Valverde observes, interdisciplinary legal studies are too often unidirectional; they seek to 'save' law from sterile doctrinalism by subjecting it to the latest in social theory without asking how legal scholarship might cross-fertilise those other disciplines.[39] In the remainder of this section, we seek to explore how legal concepts—in this case, jurisdiction—might help to explain cyberspace itself.

A brief review of sovereignty and territoriality

Because the regulation of cyberspace entails the extension of claims of sovereign authority into a new 'territory', it is convenient to reflect briefly on the relationship between sovereignty and territory, which are essentially coupled in the Westphalian paradigm. J.H. Jackson cites the conventional position as described by a US official:

> Historically, sovereignty has been associated with four main characteristics: First, a sovereign state is one that enjoys supreme political authority and monopoly over the legitimate use of force within its territory. Second, it is capable of regulating movements across its borders. Third, it can make its foreign policy choices freely. Finally, it is recognized by other governments as an independent entity entitled to freedom from external intervention.[40]

These four attributes—internal authority, border control, policy autonomy, and non-intervention—are all being challenged in unprecedented ways. One of them is surely the aspects of 'globalisation' facilitated by quick, cheap, and reliable Internet-based communications. The innovations of the digital age have accentuated the limitations of sovereignty to deal with the globalisation of financial markets. Its traditional attributes are inadequate to deal with financial conglomerates, complex groups and, generally, with cross border institutions and markets.[41]

At first blush, the concept of sovereignty would appear ill-suited to non-territorial contexts, which is probably why the cyber-sovereignty movement adopted a spatial metaphor to understand Internet communications in the first place. From a more conventional statist perspective, control over the actions of Internet participants would seem to be a matter solely for the territorial sovereigns under which those participants (physically) live, or a matter of personal jurisdiction asserted extra-territorially.

We think that a more nuanced concept of sovereignty will emerge as theories of Internet jurisdiction unfold. Too often, classical legal concepts are taken as ahistorical. This can lead to an anachronistic view of those concepts themselves. One feature of the intellectual history instructive in this context is the role of technologies used for representing reality. According to Jordan Branch, advances in cartography pre-dated and causally influenced conceptions of

---

[39] M. Valverde, 'Analysing the Governance of Security: Jurisdiction and Scale' (2008) 1 *Behemoth: A Journal on Civilisation* 3, 5.

[40] J.H. Jackson, 'Sovereignty—Modern: A New Approach to an Outdated Concept' (2003) 97 *American Journal of International Law* 782, 786, citing R.N. Haass.

[41] T. Cottier, J.H. Jackson and R.M. Lastra, *International Law and Financial Regulation in Monetary Affairs* (Oxford University Press, 2012), 417, 419.

'sovereign space'. Mapping technology made the notion of absolute, homogenous sovereign territories with contiguous, non-overlapping borders possible long before rulers actually asserted modern territorial sovereignty. Sovereign territories were conceptualised and represented as non-contiguous 'islands' of authority based around towns and cities; overlapping zones and interstitial spaces were common.[42]

Paradoxically, international private law is generally interpreted, from the perspective of Western modernity, through the lens of sovereign territorial jurisdiction and comity between nations. But the system—and much of the substance—of international private law evolved during the middle ages when no nation states existed, and when debates about sovereignty were between the Holy Roman Emperor and the Pope.[43] (Only later did European princes adopt the rhetoric of absolute power to bolster their claims for regional independence in matters of religion and more broadly; later still the rhetoric was taken up in the name of the 'people').[44] The background assumption by all the classical medieval works on the conflict of laws, whose substantive work early modern and then modern writers more or less adopted, was of a universal *ius commune*—the choice of law rules guided choices between the particular rule-sets that formed islands in a sea of interstitial common law.

Technologies, then, both undermine conventional concepts and enable rulers to stake new claims. Today, the role of local and 'private' organisations and the possibility of interstitial spaces are characteristic features of cyberspace.[45] The development of cyberspace may create the need to consider the notion of sovereignty independently of territory and, according to some views, requires the developments of a body of transnational law.[46]

In his seminal examination of the concept of sovereignty, Jackson offers a modern concept that moves away from the traditional notion of the state monopoly on power and focuses instead on the *allocation of legal authority*: '[W]hen someone argues that the United States should not accept a treaty because that treaty infringes upon US sovereignty, what the person most often means is that he or she believes a certain set of decisions should be made, as a matter of good governmental policy, at the nation-state (US) level, and not at the international level.'[47] This approach rightly focuses on the human institutions to which authority over a certain subject-

[42] J. Branch, 'Mapping the Sovereign State: Technology, Authority, and Systemic Change' (2011) 65(1) *International Organisation* 1.

[43] J. Gordley, 'Extra-Territorial Legal Problems in a World Without Nations: What the Medieval Jurists Could Teach Us' in in G. Handl, J. Zekoll and P. Zumbansen (eds.), *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (Brill 2012), 35, 41.

[44] See broadly M. Wilks, *The Problem of Sovereignty in the Later Middle Ages: The Papal Monarchy with Augustinus Triumphus and the Publicists* (Cambridge 1963).

[45] See eg E. Noor, 'The fuzzy logic of cyberspace' (*New Straits Times*, 2 June 2007), https://www.nst.com.my/opinion/columnists/2017/06/244959/fuzzy-logic-cyberspace.

[46] However see T. Forsberg, 'Beyond Sovereignty, Within Territoriality: Mapping the Space of the Late-Modern (Geo) Politics' (1996) 31(4) *Cooperation and Conflict* 355.

[47] Jackson, above n 40, 791.

matter ought to be allocated.[48] In the context of cyberspace, Jackson's analysis suggests that we need a sensitivity to the possibilities of governance at the national, but also international and sub-national level. This multi-level governance approach—which has been applied in the field of trade—is particularly suitable for the regulation of modern financial markets.[49]

Central to the question of power-allocation is the question of legitimacy, of why this institution, rather than that one, is tasked with creating and/or enforcing rules in a particular domain of social life. Reed and Murray suggest that each state, in addition to the community of residents in its territory, has an extended community in cyberspace—as they engage in different online activities, individuals enter and leave different extended communities.[50] To the extent that the source of the law's authority is the political will of the community it regulates, then, cyberspace-based communities can indeed generate legitimate normative systems. Conversely, territorial sovereigns can make legitimate claims on Internet-based actors regardless of their physical location, provided certain conditions of legitimacy are met.

In the European Union, the principle of subsidiarity in turn operates to guide these sorts of decisions; authority should be delegated to the institutions closest to the people actually subject to the authority. Adopting a framework of *cyber-subsidiarity*, instead of cyber-sovereignty, would in our opinion serve the agenda of reasonable Internet libertarians better, and may help the rest of us achieve a rational governance structure for cyberspace as well. Subsidiarity is a fundamental piece in the design of Europe's multi-level governance system of financial regulation. Cyber-subsidiarity could thus provide an anchor for a 'third way' in the regulation of cyberspace in general and Fintech in particular, a third way which is different from the statist interventionist model on the one hand and from the purely libertarian and commercial approach on the other hand.[51]

THE THIRD BORDER: CYBERSPACE

As an environment framed by physical and non-physical components, including a global network of digital computers accessible remotely, cyberspace poses an implicit challenge to the state-centric ideas of global governance.[52] Many early accounts described cyberspace as a realm completely apart from physical reality, in order to bolster a claim of cyber-sovereignty. The thrust of Johnson and Post's 1996 argument, for example, was that the assertion of territorial jurisdiction over Internet-based information flows could not govern cyberspace

[48] Reed, above n 10, 25.

[49] Cottier, Jackson and Lastra, above n 41, 413, 415 and ch 8; see also T. Cottier, 'Constitutionalism, Multilevel Trade Governance and Social Regulation' (2006) 10(2) *Journal of International Economic Law* 554.

[50] C. Reed and A. Murray, *Rethinking the Jurisprudence of Cyberspace* (Edward Elgar 2018), 18.

[51] J. Thornhill, 'There is a third way for Europe to navigate the digital world', *Financial Times*, 19 November 2018, URL: https://www.ft.com/content/9da4156c-ebd4-11e8-89c8-d36339d835c0

[52] A.N. Liaropoulos, 'Cyberspace Governance and State Sovereignty' in G.C. Bitros and N.C. Kyriazis (eds.), *Democracy and an Open-Economy World Order* (Springer 2017), 25.

effectively.[53] This ontological 'place-ness' argument served the normative argument that cyberspace ought to be allowed to create its own normative order(s), and that 'virtual jurisdictions' ought to be treated like territorial jurisdictions in being allowed to create divergent rule-sets. Perhaps because commentators have tended to conflate the descriptive aspect of the metaphor and its normative implications, the notion of cyberspace as a place has remained controversial.[54] As long as its limitations as a metaphor are acknowledged, however, we think it is descriptively useful, and that it does not commit us to such a normative project.

Positions in the contemporary Internet jurisdiction debate offer different answers to the questions whether Internet-based activities should be governed at all and who should govern them (particularly, what role different actors including firms, non-governmental organisations, nation states, and supra-national organisations should play in that governance). Views range from Internet anarchism to the complete subordination of the Internet to national jurisdiction through the creation of national Intranets.[55] Taking a multi-lateral governance approach, conventional state sovereigns have a distinct and essential role to play, but a legitimate role exists for private and quasi-public actors, as well.[56] In our view, national 'law spaces' will remain important in the sphere of financial regulation, and this makes it crucial to map the relation between conventional territorial jurisdictions and cyberspace.

Our main objective is to present a set of methodological considerations that we think frame the debate in the context of financial services. The starting point, again, is cyberspace *qua* place. Returning to Johnson and Post, the 'new boundary', they claimed, 'is real':

> Traditional legal doctrine treats the Net as a mere transmission medium that facilitates the exchange of messages sent from one legally significant geographical location to another, each of which has its own applicable laws. But trying to tie the laws of any particular territorial sovereign to transactions on the Net, or even trying to analyse the legal consequences of Net-based commerce as if each transaction occurred geographically somewhere in particular, is most unsatisfying. A more legally significant, and satisfying, border for the 'law space' of the Net consists of the screens and passwords that separate the tangible from the intangible world… There is a 'placeness' to Cyberspace because the messages used there are persistent and accessible to many people.[57]

It is helpful, again, to reject the opposition of 'cyberspace' and the 'world of atoms' to the extent it encourages an opposition of the 'digital' and the 'real'. A large part of the real is

[53] See Johnson and Post, above n 8, 1370-1378. See *contra* J.L. Goldsmith, 'Against Cyberanarchy' (1998) 65 *University of Chicago Law Review* 1199. See also J.A.T. Fairfield, 'The Magic Circle' (2009) 11 *Vanderbilt Journal of Entertainment and Technology Law* 823, 828.

[54] Hunter, above n 7, 443; Johnson and Post, above n 8, 1387, 1400.

[55] Liaropoulos identifies three main models: 'distributed governance', 'multilateral governance', and 'multi-stakeholderism'. Liaropoulos, above n 52, 27.

[56] See R.M. Lastra and J.G. Allen, above n 15, 15. See also R. Schu, 'The Applicable Law to Consumer Contracts Made Over the Internet: Consumer Protection Through Private International Law?' (1997) 5(2) *International Journal of Law and Information Technology* 192; A. Manolopoulos, 'Raising "Cyber-Borders": The Interaction Between Law and Technology' (2003) 11(1) *International Journal of Law and Information Technology* 40; L.E. Gillies, 'Addressing the "Cyberspace Fallacy": Targeting the Jurisdiction of an Electronic Consumer Contract' (2008) 16(3) *International Journal of Law and Information Technology* 242.

[57] Johnson and Post, above n 8, 1378, 1379.

digital, and is now 'located' in cyberspace; the border between cyberspace and the real world is not a border between an *informational domain* and a *physical domain*, but between official projections of legal and economic institutional reality and an undefined mass of online social interactions of uncertain legal status (from the point of view of any legal system). To understand this border, it is necessary (i) to understand the nature of conventional legal reality and (ii) to understand the physical footprint of cyberspace and its users. We will take those questions in order, dealing with (ii) in the next section. Here, we set out our framework for understanding conventional legal reality.

In one of the first efforts to describe the ontology of cyberspace with a legal focus, David Koepsell rightly observed that the ontology of the *law* has not yet been adequately theorised.[58] How is it that invisible, intangible objects such as legal rights or digital financial records assume 'reality'? How are they created and maintained, and how are they distinguished from, for example, 'rights' and 'duties' in a game, or electronic 'money' and 'securities' on a simulated trading platform?[59] Most of law's stock-in-trade is invisible: you can't pack a right in a box; as Coffee put it, a corporation has 'No Soul to Damn: No Body to Kick'.[60] When a regime changes, entities—from land titles to public debt instruments to units of money—are liable simply to disappear with it (subject to rules of state succession). The same is true of borders: one of us walks past Checkpoint Charlie every day.

The socially-constituted objects, which are often themselves intangible, exist because we *document* their existence—with treaties, lease agreements, marriage certificates, letters patent, debentures, certificates of incorporation, acts of parliament, judgments, affidavits, and tax assessments, we create vast and complex structures within institutional legal reality.[61] Barry Smith argues, in terms that mirror Johnson and Post's emphasis:

> A document is something that is able to *endure self-identically through time*. It can be signed and countersigned, stored, registered, inspected, conveyed, copied, ratified, nullified, stamped, forged, hidden, lost or destroyed. Pluralities of documents can be chained together … and combined in other ways to form new document-complexes, whose structures mirror underlying human relations for example of debtor to creditor, of manager to shareholder, of customer to supplier… *Documents thereby make possible new kinds of enduring social relations and new kinds of enduring social entities together allowing the evolution of entire new dimensions of socio-economic reality.*[62]

---

[58] D. Koepsell, *The Ontology of Cyberspace: Ontology, Law, and the Future of Intellectual Property* (Open Court 2000), 14.

[59] See J.G. Allen, 'Property in Digital Coins' (2019) 8(1) *European Property Law Journal* 64; J.G. Allen, 'Law's Virtual Empires: Games Analogies and the Concept of Law' G. Villa Rosas and J. Fabra Zamora (eds.), *New Directions in the Concept of Law* (forthcoming Springer 2020).

[60] See J.C. Coffee, Jr., '"No Soul to Damn: No Body to Kick": An Unscandalized Inquiry into the Problem of Corporate Punishment' (1981) 79(3) *Michigan Law Review* 386, quoting Thurlow LC's proverbial complaint.

[61] See B. Smith, 'How to Do Things with Documents' (2012) 50 *Revisti di estetica* 179; D. Koepsell and Barry Smith, 'Beyond Paper' (2014) 97(2) *The Monist* 222; M. Ferraris and G. Terrengo, 'Documentality: A Theory of Social Reality' (2014) 57(3) *Revisti di estetica* 11; M. Ferraris (R. Davies trans.), *Documentality: Why it is Necessary to Leave Traces* (Fordham University Press 2012).

[62] Smith, 'How to Do Things with Documents', above n 61, [11]. Emphasis ours.

Even territorial jurisdictions are created (and changed) through *speech-acts*, usually recorded in documents—declarations of independence, constitutions, town charters, planning applications, etc. These documentary utterances create the politico-legal geography of the world around us.[63] Only in the second instance are walls and checkpoints constructed to mark their borders.[64]

Thus, the notion that cyberspace acquires 'place-ness' by virtue of the fact that messages accessed there are persistent over time, and are accessible to many people regardless of physical location, may be a metaphor—but it is a useful one. As Dan Hunter has argued, evidence from cognitive science has convincingly demonstrated that we do actually think about cyberspace as a place. Even those sceptical of the place metaphor 'find it impossible to talk about Internet regulation without invoking spatial references,' and it has become common to map non-Cartesian, abstract 'spaces'.[65] In our view, the metaphor aptly expresses the role of communications and documents in the ontology of social reality.[66] These invisible objects, events, and actions structure our social lives. A significant part of our lives as human beings is not composed of physical interactions at all, but of institutional interactions that are mediated by language and made possible by the existence of rules.[67] Ultimately, they help to structure the interactions between physical human bodies and physical objects in the world of atoms.

What we are witnessing now is a rapid expansion in the scale of Smith's 'document-complexes' (structured aggregations of institutional documents) riding on the back of developments in ICT. First computers, then computer networks (notably the Internet) and now new data structures within those networks (notably DLT) have made novel document-complexes possible. When these new document-complexes are treated as real by market participants, they assume a degree of social reality, just like their paper forebears.[68] True, there may be ontologically relevant differences between paper-based and digital documents;[69] we could anchor physical documents in the 'real world' (ie, the parts of social reality that we conventionally regard as self-evident) by virtue of their physical embodiment, and we could place digital documents in 'cyberspace' because they exist in a different medium. But it is also important to recognise that both belong

[63] See Robinson, above n 32.

[64] Using the *pomerium* example, and Romulus' killing of Remus for mocking his work, see D. von Daniels, 'Normativity and the Sources of International Law' in Samantha Besson und Jean d'Aspremont (eds.), *The Oxford Handbook on the Sources of International Law* (Oxford University Press 2017).

[65] Hunter, above n 7, 443, 455, 457, 458; see eg W.J. Mitchell, *City of Bits: Space, Place, and the Infobahn* (MIT Press 1995).

[66] Johnson and Post, above n 8, 1379; see also D.H. Holmes, 'Economy of Words' (2009) 24(3) *Cultural Anthropology* 381; D.A. Westbrook, 'Magical Contracts, Numinous Capitalism' (2016) 32(6) *Anthropology Today* 1.

[67] See eg, I. Reiland, 'Constitutive Rules: Games, Language, and Assertion' (2017) *Philosophy and Phenomenological Research*, https://doi.org/10.1111/phpr.12525.

[68] See eg, M. Hildebrandt, 'Law *as* Information in the Era of Data-Driven Agency' (2016) 79(1) *The Modern Law Review* 1, 1.

[69] See J.S. Rogers, 'An Essay on Horseless Carriages and Paperless Negotiable Instruments: Some Lessons from the Article 8 Revision' (1995) 31 *Idaho Law Review* 689, 690.

to a reality that is mediated and facilitated by information technology. For all the novelty of DLT (for example), the history of finance is full of examples of market innovation leading regulation, taking advantage of new technologies.[70]

Current developments are challenging for the traditional paradigm of territorial regulation because, where paper documents have a physical existence and have to be stored somewhere, the Internet, cloud-based storage, and DLT *attenuate the link between political geography and institutional legal reality*. Things seem to float in a parallel realm, accessible by everyone at all times irrespective of their geographical location (or the jurisdiction in which that geographical location lies). Of course, there are physical barriers to accessing the Internet: More than a billion people live behind a state-imposed firewall,[71] and billions still lack access to the internet for want of a connection, an Internet-capable device, or electricity to charge it.[72] Furthermore, the Internet has a physical footprint (server farms and undersea cables), as do its human users. One aspect of our border, then, would appear to be a border between *abstraction* and *materially-embodied abstraction*, in the sense of the point in space and time at which systems of symbols (ie computer languages) interact with physical hardware systems (ie computers).[73] But this is not the same as the intuitive border between 'cyberspace' and the 'world of atoms'. The border is one between *two sub-domains of technologically-mediated social reality*. While it would be unwise to posit that cyberspace should be treated as an extension of a jurisdiction straightforwardly, then, cyberspace might be the context for a refinement or redefinition of the concept of territorial jurisdiction in the future.

GUARDING THE THIRD BORDER

Accepting the metaphor of cyberspace heuristically, we now consider how national jurisdictions guard themselves against risks that have their source in Internet-based financial activities.

Incorporation: Border-crossing or land grab?

As we mentioned at the outset, cyberspace provides a *situs* for objects, events and actions that are sometimes, but not always, given relevance in legal institutional reality. When one transfers demand deposits in a bank account held in one's name to a bank account in another's name, for example, the legal system deems a relevant action to have taken place, such as the satisfaction of a debt. Legal theory, however, has not done a very good job of mapping this

[70] See P. Ireland, 'Capitalism without the capitalist: The joint stock company share and the emergence of the modern doctrine of separate corporate personality' (1996) 17(1) *The Journal of Legal History* 41.

[71] See eg E.C. Economy, 'The great firewall of China: Xi Jinping's internet shutdown' (*The Guardian*, 29 June 2018), https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

[72] See eg https://www.statista.com/topics/1145/internet-usage-worldwide/ (as at 27.08.2018).

[73] See R. Abbott, 'The Bit (and Three Other Abstractions) Define the Borderline Between Hardware and Software' (2019) *Minds and Machines* DOI: https://doi.org/10.1007/s11023-018-9486-1.

familiar terrain; international private law, for example, puzzles over questions such as 'Where is a bank account?'[74] and 'Where is a debt?'.[75] Such questions are acute given the ubiquity of digital record-keeping, and aggravated by cloud computing and DLT.

Fundamentally, cyberspace would be irrelevant if the objects, events, and actions in it were not given relevance by the legal system.[76] A dollar of commercial bank 'book money', a bitcoin, and a coin of *World of Warcraft* gold are the same in many ontological respects. Their data structure and manner of storage differ, but they are all constructed purely of data that represents relations between actors. The difference is that a legal system *positions* them differently, ie, imposes a different status on them.[77]

When we speak of cyberspace in the context of the shadow financial system, we are speaking of objects, events, and actions in cyberspace which a legal system positions as 'real'. An insight from the literature of legal pluralism is apposite here. Different legal systems create different *legal objects* upon the same *social objects*; one legal system will regard a piece of paper as a 'deed', for example, while another may not. In effect, legal status represents a distinct ontological layer. For example, a marriage may be valid (exist) as a matter of customary law, and may be recognised by some state laws but not by others. Different spheres of legality operate at different scales—local, regional, national, transnational, imposing their meanings on the social worlds with which they interact.[78] In order to say what a certain thing *is*, it is therefore necessary to adopt a 'law space' as the place from which to observe it. Our default position is, say, that of the official state law of a Member State of the European Union. But transnational capital has long created its own sphere of legality, eg the *lex mercatoria* of the middle ages or the customs, standards, and contractual frameworks of the current day, that operate with some degree of efficacy in parallel to state law, and the *lex financiera* that has emerged more recently.[79]

'Incorporation' of a social object into a catalogue of recognised legal objects seems to be a fact-driven phenomenon. The law often follows the market; when (enough) market participants attribute real world value to a cyber-object, the border is crossed. For example, there are instances of national courts treating *World of Warcraft* artefacts as 'property' capable of theft.[80]

---

[74] J.H. Sommer, 'Where is a Bank Account?' (1998) 57(1) *Maryland Law Review* 1.

[75] P.G. Rogerson, 'The *Situs* of Debts in the Conflict of Laws: Illogical, Unnecessary and Misleading' (1990) 49 *Cambridge Law Journal* 441; —, 'Jurisdiction and the "*Situs*" of Debts' (1925) 34(6) *Yale Law Journal* 652.

[76] A 'magic circle' separates the game world from the real world. However, see Fairfield, above n 53.

[77] See eg Tony Lawson, 'The Constitution and Nature of Money' (2018) 42(3) *Cambridge Journal of Economics* 851.

[78] See B. de Sousa Santos, 'Law: A Map of Misreading. Toward a Postmodern Conception of Law' (1987) 14(3) *Journal of Law and Society* 279, 287.

[79] On the development of a new *lex financiera*, see Lastra, above n 28, 522; on the parallels between the *lex mercatoria* and the *lex cryptographica*, see De Filippi and Wright, above n 11, ch 11 and ch 12.

[80] In Taiwan, for example, virtual objects have constitute 'property' for the purposes of the law of theft since 2001; see Taiwan Ministry of Justice Official Notation No 039030, cited in Joshua Fairfield 'Virtual Property'

While this is contentious in the context of games,[81] a functional approach seems sensible when considering innovations in digital financial transactions. Whenever events in unregulated cyberspace could destabilise the regulated economy of territorial political community, for example, it is *prima facie* a matter of interest to that community's regulatory authorities. It would be foolish to say that an objects does not exist when it poses financial stability risks. For example, where a regulated financial entity takes a position in cryptoassets such that it would suffer liquidity problems if the USD to Bitcoin exchange rate shifted, the 'third border' is crossed, even though national regulators may not have taken an official stance on Bitcoin or other cryptocurrencies. In this context, the problem of access to lender of last resort or other crisis management instruments constitutes, together with the issues of consumer protection and dispute resolution (appeal mechanisms), major challenges of the market in cryptoassets and Fintech more broadly.

This border crossing, however, could also be characterised as a 'land grab'. When an object is incorporated, the sovereign recognising it is asserting jurisdiction over a 'patch' of cyberspace. As noticed above, it would be possible to collapse all three borders conceptually into one, ie, the border between the regulated and the unregulated. Indeed, much can be done to enforce the first border by extending it to include objects, events and activities that exist in cyberspace. This approach has characterized the first wave of responses to cryptoassets.[82]

The empire strikes back?

Cyberspace can be used to evade laws. The use of Bitcoin (for example) to facilitate illegal activities is well-documented. But, after the first wave of libertarian literature, scholars began to observe that the affordances of digital environments can also enable national governments to enforce their laws.[83] Devices such as data retention, geo-location and filtering can be employed to emulate territorial space in cyberspace and to block or channel Internet traffic (at least for less sophisticated users). As Joachim Zekoll observes, such devices not only recreate and reinforce national borders, but can be more effective than real world enforcement because—harking back to our discussion of Lessig, above—prohibited actions can be

(2005) 85 *Boston University Law Review* 1047, 1086. See also F.G. Lastowka and Dan Hunter, 'Virtual Crimes' in J.M. Balkin and B.S. Noveck, *The State of Play: Law, Games, and Virtual Worlds* (NYU Press 2006).

[81] Some argue that the 'magic circle' excluding game objects from the real-world economy must be maintained in order to protect the right to play: See E. Castranova, 'The Right to Play' in J.M. Balkin and B.S. Noveck, *The State of Play: Law, Games, and Virtual Worlds* (NYU Press 2006), 68.

[82] See generally A. Blandin *et al*, above n 5. See eg, Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Release No. 81207, 25 July 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf; *Commodities Futures Trading Commission v Patrick K. McDonnell and Cabbagetech Corp t/a Coin Drop Markets*, Memorandum & Order of the US District Court, Eastern District of New York 18-CV-361, 3 June 2018, URL: https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf.

[83] See J. Zekoll, 'Jurisdiction in Cyberspace' in G. Handl, J. Zekoll and P. Zumbansen (eds), *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (Brill 2012), 344, citing Horatia Muir Watt, Lillian Edwards, and Lawrence Lessig.

automatically rendered impossible in the digital environment. To the extent this occurs, he observes, 'it entails the Balkanisation of the Internet through the instant enforcement of state interests with regard to constitutional values, political and economic goals and social content.'[84] In our view, the goals of consumer protection and financial stability present two such goals that could plausibly justify the extension of more robust sovereign claims into cyberspace.

D.G. Post has conceded, in a more recent contribution, that apparently 'territory-defying' technologies are, paradoxically, making jurisdiction more important than ever. The possibility of action at a distance, and the 'convulsive rescaling' of the social and economic world it causes, challenges the conventional framework of territorial jurisdiction and underscores the importance of geo-political power in our (ultimately physical) world. Although many thought that national boundaries were about to disappear in the 1990s, Post reflects that currently 'more resources than ever are being diverted to shoring them up.'[85] A debate on Internet jurisdiction, he predicts, is about to begin in earnest.[86] The crux of the debate is the juxta-position of non-territorial *fora* for economic activity, on the one hand, and territorial concentrations of politico-legal power, on the other. He cites C.S. Maier's observations on the importance of the third border in the grand sweep of modern history:

> [The] spread of these new technologies] transforms the major political division of our times into one that separates those who envisage their future prospects based on non-territorial markets and the exchange of ideas from those who insist that territoriality can be reinvigorated once again as the basis for economic and political security—whether by means of provincial regionalism, or supranational organization, or by harsher measures of ethnic homogeneity.[87]

We are concerned, then, with the changing relations between 'law' (as conventionally understood through the framework of the territorial nation state) and a political economy that is globalising rapidly, not least through developments in ICT.[88] These relations again problematise conventional assumptions about territoriality and jurisdiction.

Cyberspace as a source of risk to the financial system

It is helpful to ground complex discussions, like that around Internet jurisdiction, in a concrete problem. The debate takes on particular nuances in the context of financial services, on which we focus the rest of this article. The objectives of financial stability and consumer protection help to frame the question of jurisdiction over Internet-based financial services and, we suggest, delimit the appropriate extent of state intervention in this context. (We leave aside in

[84] *ibid*.

[85] See Post, above n 37, 253, 255.

[86] *ibid*, 257-258.

[87] C.S. Maier, 'Consigning the Twentieth Century to History: Alternative Narratives for the Modern Era' (2000) 105(3) *The American Historical Review* 807, 824.

[88] See P. Zumbansen, 'Defining the Space of Transnational Law: Theory, Global Governance, and Legal Pluralism' (2012) 21 *Transnational Law and Contemporary Problems* 305, 307.

our discussion in this article other important financial regulatory goals such as market integrity or combating money laundering).

The concept of financial stability has gained in relevance in recent years, although it has a long-standing tradition in central banking often under other names, such as sound banking. It was somewhat 'rediscovered' following the GFC. As a goal for financial regulatory authorities, however, financial stability is difficult to define and is often more identifiable in its negative definition (ie, 'what is instability?') than in its positive definition. At base, it is concerned with avoiding systemic risk and building systemic resilience; financial stability, systemic risk, contagion control, and sound banking are 'close cousins'. What is clear, though is that financial stability complicates border problems because it transcends institutional mandates[89] and geographical boundaries, thus further challenging the traditional notion of sovereignty. Financial stability is indeed a national, regional and international goal; episodes of instability, like tsunamis and epidemics, do not respect territorial boundaries. *Pace* Sheldon and Maurer:

> Systemic risks are for financial market participants what Nessie, the monster of Loch Ness, is for the Scots (and not only for them): Everyone knows and is aware of the danger. Everyone can accurately describe the threat. Nessie, like systemic risk, is omnipresent, but nobody knows when and where it might strike. There is no proof that anyone has really encountered it, but there is no doubt that it exists.[90]

In a joint document published by the International Monetary Fund, the Bank for International Settlements and the Financial Stability Board in response to a G-20 mandate, systemic risk in financial markets is defined as 'the risk of widespread disruption to the provision of financial services that is caused by an impairment of all or parts of the financial system, which can cause serious negative consequences for the real economy'.[91] Negative externalities (contagion) are key to its understanding. Philip Davis has defined systemic risk as a 'disturbance in financial markets which entails unanticipated changes in prices and quantities in credit or asset markets, which lead to a danger of failure of financial firms, and which in turn threatens to spread so as to disrupt the payments mechanism and capacity of the financial system to allocate capital.'[92] Other definitions also point to the probability of breakdown in the entire financial system, as opposed to breakdowns in individual parts or components. According to Hal Scott, systemic risk is *'*the risk that a national, or the global, financial system will break down*'*.[93]

---

[89] For example, in the US, the post-GFC Dodd-Frank Act 2010 establishes *inter alia* a Financial Services Oversight Council ('FOSC') with eight members made up from the heads of each of the principal federal financial regulators, replacing the President's Working Group on Financial Markets.

[90] G. Sheldon and M. Maurer 'Inter-Bank Lending and Systemic Risk: An Empirical Analysis for Switzerland' (1998) 134 *Swiss Journal of Economics and Statistics* 685, 685.

[91] 'IMF-FSB-BIS Elements of Effective Macroprudential Policies. Lessons from International Experience'(IMF 2016), URL: https://www.imf.org/external/np/g20/pdf/2016/083116.pdf, 4. See also https://www.bis.org/publ/othp07.pdf; https://www.imf.org/external/np/pp/eng/2013/061013b.pdf; https://www.fsb.org/2011/10/r_111027b/ and https://www.bis.org/publ/cgfs38.pdf

[92] P. Davis, *Debt, Financial Fragility and Systemic Risk* (Clarendon Press, 1992), 117.

[93] H. Scott, 'Reducing Systemic Risk Through the Reform of Capital Regulation' (2010) *13 (3) Journal of International Economic Law* 763–778, 763.

While systemic risk is often associated with the contagion effect triggered by default or credit risk, in our opinion any risk—including liquidity risk, market risk, legal risk, operational risk—can grow to systemic proportions when its negative impact extends beyond an individual institution and affects or threatens to affect other institutions, leading to a disruption in the financial and payments systems and even the economy at large. For example, consider an unregulated Internet-based payments provider. If this provider were to experience liquidity problems, it could affect users' ability to meet their obligations with impacts throughout the broader ('real') economy.

Central to the idea of systemic risk post-GFC is the concept of Systemically Important Financial Institutions ('SIFI'). SIFIs are entities that are so important for the functioning of a financial system that their problems—and, in particular, their failure—can trigger system-wide problems, because they are 'too big to fail', 'too interconnected to fail', or 'too significant to fail'.[94] SIFIs present additional challenges to the delimitation of borders because the Internet offers unparalleled opportunities for circumventing financial regulations such as those identifying and controlling SIFIs.[95] As Goodhart and Lastra observe, vulnerability to 'gaming' is an inherent feature of regulation itself:

> In so far as regulation is effective in forcing the regulated to shift from a preferred to a less desired position, it is likely to set up a boundary problem. It is, therefore, a common occurrence, or response, to almost *any* regulatory imposition. A current [2010] example is the proposal to introduce additional regulatory controls on systemically important financial intermediaries (SIFIs). If SIFIs are to be penalized, there needs, on grounds of equity and fairness, to be some definition, some criteria, of what constitutes a SIFI, an exercise with considerable complication. But once such a definition is established and a clear boundary established, there will be an incentive for institutions to position themselves on one side or another of that boundary, whichever may seem more advantageous. Suppose that we started, say in a small country, with three banks, each with a third of deposits, and each regarded as [too big to fail], and the definition of a SIFI was a bank with over 20% of total deposits. If each bank then split itself into two identical clones of itself, to avoid the tougher regulation, with similar portfolios and interbank linkages, would there have been much progress? Similarity can easily generate contagion. Indeed, regulation tends to encourage and to foster similarity in behaviour.[96]

From this aspect, borders appear almost like a resource that actors can mobilise in both good and bad faith.[97] Insofar as actors attempt to avoid triggering SIFI regulations, but remain *de facto* of systemic importance, such regulations could in fact increase systemic risk rather than mitigating it. The 'third border' offers actors new opportunities for structuring transactions and relationships to avoid moving into the regulated space. This points, again, to the utility of the

---

[94] See eg the so-called 'Geneva Report' by M. Brunnermeier, A. Crocket, C.A.E. Goodhart, A. Persaud and H. Shin, 'The Fundamental Principles of Financial Regulation', *Geneva Report on the World Economy* (February 2009). See also Goodhart and Lastra, above n 1.

[95] This has become known as 'Goodhart's Law'. See C.A.E. Goodhart, 'Problems of Monetary Management: The U.K. Experience' in A.S. Courakis (ed.), *Inflation, Depression, and Economic Policy in the West* (Rowman & Littlefield 1981), 111.

[96] See Goodhart and Lastra, above n 1, 712-713.

[97] See C. Sohn, 'Modelling Cross-Border Integration: The Role of Borders as a Resource' (2014) 19(3) *Geopolitics* 587.

borders metaphor to understand not only the need for regulation but the intended and unintended impacts of regulation, including substitution flows.

The definition of a systemically significant financial institution is also dynamic. What is systemic today will not necessarily be systemic tomorrow. Indeed, the lists of SIFIs are frequently being revised. A new taxonomy is now applicable to those entities that can create systemic risk according to their line of financial business (G-SIBs or Global Systemically Important Banks and G-SIIs or Global Systemically Important Insurers) and according to their relevance nationally or internationally.[98] The fact that most SIFIs have a cross-border presence and a cross-border dimension to their business calls, in our view, for a cross-border solution involving supra-national or international coordination of conventional sovereign states. The third border adds a further layer of complexity to the regulatory treatment of SIFIs, since national solutions alone will not suffice to prevent and contain systemic risk. However, again, cooperation between states logically presupposes and practically relies on national territorial jurisdiction.

The notion of 'scaling' is instructive in this context. Harking back to our discussion of Jackson, above, part of the question of *how* risks should be regulated is *who* should regulate them, and one's answer to this question rests on assumptions one makes about the scale of the relevant space. According to Valverde:

> Some risks are thought of as essentially global, others as national, and others yet as local: these shifts in scale are incorporated, usually without much discussion, into security strategies. […] By contrast, political and legal theory habitually privilege the scale of the nation-state. […] Political and legal theory work almost wholly with two scales only, the national and the transnational/global.[99]

These assumptions, in turn, directly inform arguments about the proper location of regulation—where, in effect, the border should be raised. Avoiding the twin risks of Balkanisation and a race to the bottom (which encourages jurisdictional arbitrage), we agree that new, hybrid modes of governance may need to emerge for the effective and compelling regulation of financial services in cyberspace.[100]

Jurisdiction in 'cyber-territories'

---

[98] The FSB, in consultation with the International Association of Insurance Supervisors (IAIS) and national authorities, began identifying global systemically important insurers (G-SIIs) in 2013. The list is available at https://www.fsb.org/2017/11/review-of-the-list-of-global-systemically-important-insurers-g-siis/. The list of Global Systemically Important Banks is available at https://www.fsb.org/wp-content/uploads/P161118-1.pdf. In the Eurozone, the ECB uses the test of significance in terms of relevance for the national economy of the participating Member State according to Article 6(4)(2) of the SSM regulation. In the US, Section 113 of the Dodd-Frank Act 2010 gives the FSOC the power to determine SIFIs within the territory of the USA and to bring them under the supervision of the Federal Reserve Board if FSOC determines that 'material financial distress at the US nonbank financial company, or the nature, scope, size, scale, concentration, interconnectedness, or mix of the activities of the US nonbank financial company, could pose a threat to the financial stability of the United States.'

[99] Valverde, above n 39, 2.

[100] This argument is developed and extended in Reed and Murray, above n 50.

Legal systems take a variety of approaches to establishing jurisdiction in cases where the matter of a transaction has a connection with more than one jurisdiction. Choice of law rules, for example, determine the proper law of a contract or a tort by reference to the nationality and residence of the parties involved, the place in which the operative events occurred, and the place in which the relevant objects are situated. But these rules evolved in the era of territorial jurisdiction—pre-Fintech, Fintech 1.0 and early Fintech 2.0. They do not always apply straightforwardly to Fintech 3.0.[101] For example, the idea that a bank account has a *situs* was difficult enough in the era of paper book-keeping.[102] Things are only more complicated today.

The ultimate task is to develop a theory of Internet jurisdiction that explains the application of law to persons acting in cyberspace and to the 'natively digital' objects they act upon. Mindful of a metaphor's limits, the borders metaphor invites a few useful questions. Is cyberspace like a newly discovered continent, an America ready to be carved up by existing geo-political players? Or is it more like the high seas which are, by their nature, beyond the kind of control that makes conventional sovereignty possible? Should conventional sovereigns attempt to 'occupy' cyberspace right up to contiguous and non-overlapping borders, or respect interstitial spaces? What role does technological constraint, as opposed to conventional norms, play in the governance of this space? Should the emerging normative framework be seen as a 'pirate code', a modern body of custom like the medieval *lex mercatoria*, a body of 'transnational pluralist law', or a branch of international law made by sovereign states?[103] What is the importance of community; what space do non-state associations occupy in this landscape; and how much political 'weight' should non-territorial Internet communities be given?

As a starting point, it is necessary to distinguish between the 'layers' of cyberspace, which are often neglected in legal analysis. Yochai Benkler observes (i) a *physical* layer (ie, undersea cables, computer servers, and wireless routers), (ii) a *logical* layer (ie, the rules governing access to and use of the network) and (iii) a *content* layer (ie, the content actually being communicated, such as the data packet that constitutes a US dollar or a bitcoin).[104] We would add a fourth—a *social* layer[105]—positioning banking records and bitcoins as 'real' assets and *World of Warcraft* gold as 'game' assets. The concept of jurisdiction would seem to comprise part of this fourth layer, and it interacts with the other layers in different ways. In effect, the concept of jurisdiction, when extended to non-spatial artefacts, positions those artefacts as objects with 'real world' value that the relevant authority has some valid interest in regulating.

---

[101] See C. McLachlan, 'From Savigny to cyberspace: Does the Internet sound the death-knell for the conflict of laws?' (2006) 11(4) *Media & Arts Law Review* 418.

[102] J.H. Sommer, 'Where is a Bank Account?' (1998) 57(1) *Maryland Law Review* 1, 5.

[103] See eg J.P. Barlow's 'Declaration of the Independence of Cyberspace' in Peter Ludlow (ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias* (MIT Press 2011).

[104] M.A. Geist, 'Is There a There There—Toward Greater Certainty for Internet Jurisdiction' (2001) 16(3) *Berkeley Technology Law Journal* 1345, 1354 citing Yochai Benkler.

[105] See eg R. Cooper and M. Foster, 'Sociotechnical Systems' (1971) 26(5) *American Psychologist* 467 for a review of the early literature on socio-technical systems. We use the term in a slightly different sense, inflected by more recent work in social ontology; the crux of the matter is the imposition of social meaning on technical processes.

This is illustrated by the concept of the 'magic circle' hiving game activities off from the 'real world'; game money, promises, frauds, etc, are not given the kind of value by state law that would require the assertion of jurisdiction over them—at least not until they start to affect non-game interests.[106]

According to M.A. Geist, the concept of jurisdiction comprises three layers, too: (i) the courts (and other legal institutions) that could have jurisdiction, (ii) the substantive law that they would apply, and (iii) the enforcement of legal rulings in an online environment.[107] The physical layer of the Internet is most easily brought under territorial jurisdiction; fibre-optic cables are physically located somewhere and owned by someone with a home jurisdiction. The logic layers and content layers, on the other hand, are less 'grounded'. The infrastructure of the logic layer may be in one state, but the content is accessible by (or targeted towards) users resident in another state, leading to a conflicts-type problem. The application of regulations to Internet-based financial services, then, should not only be informed by an awareness of the layers in any given case, but also the aspects of jurisdiction that are being conceptually extended to cover them.

Surveying the range of solutions in the conventional law, there is no 'silver bullet' that will solve the Internet jurisdictional problem;[108] a combination of approaches is necessary, which may evolve over time. A conventional conflicts or international private law approach is obviously essential. This allows the courts of one state to assume jurisdiction, but apply the norms of another state more appropriate to the matter.[109] But, in our view, such an analysis is insufficient on its own; there are other important aspects.[110] D.J.B. Svantesson has recently argued (correctly, in our view) that it is necessary to embrace not only conventional conflicts analyses, but international public law analyses, as well. These include, in particular, (i) the connection between the state claiming jurisdiction and the Internet-based matter, (ii) a legitimate state interest in the matter, and (iii) a balancing of that state's interest with other relevant interests.[111]

The potentially disruptive impact of Fintech on conventional notions of sovereignty is particularly important in the context of monetary policy. Claus Zimmermann has reviewed the conventional treatment of monetary sovereignty, and concludes that it is usually treated as a part of the general concept of (territorial) sovereignty that pertains to the rights and obligations of states to print money and honour monetary obligations.[112] But the concept is broader than

[106] See Allen, above n 59.

[107] Geist, above n 104 1354.

[108] S.R. Shaw, 'There is no silver bullet: solutions to Internet jurisdiction' (2017) 25 *International Journal of Law and Information Technology* 283.

[109] C. McLachlan, above n 100, 439.

[110] See J. Daskal, 'The Un-Territoriality of Data' (2015) 125 *Yale Law Journal* 326, 332.

[111] See D.J.B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford 2017), ch 3.

[112] See C.D. Zimmermann, 'The Concept of Monetary Sovereignty Revisited' (2013) 24(3) *European Journal of International Law* 797, 798; see also Lastra, above n 28, 22.

this. As Pistor argues, monetary sovereignty is a unique concept that involves a relationship of transitivity between overlapping normative, institutional practices. 'Public money' (eg, central bank issued currency) and financial instruments issued by private entities today 'form part of an integrated, hierarchical money system, both domestically and globally.'[113] The domestic and global money systems, she argues, are like interlocking balance sheets, in which one party's credit is another's debit; 'sovereignty' in a relationship like this means that a party can create the units in which its debts are payable. Sovereignty is reduced (or lost) when a nation state assumes obligations in a foreign currency. But it is also reduced whenever one entity (eg a bank) can compel another (eg a state) to provide liquidity assistance—for example, to prevent contagion spreading through the national economy in a crisis. In our view, this would provide a state with a legitimate interest in, for example, asserting a kind (or degree) of 'sovereign' jurisdiction over an Internet-based payments provider presenting a systemic risk to the national economy.

Combining these insights, a proper approach requires a granular view of cyberspace *per se* (ie looking at each of its physical, logical, and content layers) and an analysis of how each layer (i) connects an Internet-based financial object, event or action to the jurisdiction of one or more territorial sovereigns, (ii) touches the legitimate interests of one or more territorial sovereigns, and (iii) balances these legitimate interests. In the context of financial regulation, we think that states' interests must centre on (i) promoting financial stability and resilience, (ii) consumer protection and (iii) dispute settlement. These connecting factors may not apply straightforwardly; for example, a Fintech application could be designed specifically to avoid certain physical Internet infrastructure, yet still have a strong connection with some jurisdiction in virtue of the identity and location of the transacting parties. In other words, what we have called the 'social layer' of the Internet must be dispositive, because that is the ontological domain in which jurisdiction and cyberspace actually interact.

Four Internets (and a freeriding troll)

O'Hara and Hall have recently observed 'four Internets' emerging.[114] The 'Silicon Valley open Internet' reflects the idealism of the Internet's creators, who engineered it to be open, with transparent standards, portable, extensible and interoperable data and software, able to scale as it grows. The 'Brussels bourgeois Internet' is protective of privacy and discouraging of bad online behavior—even at the cost of innovation.[115] A third group, typified by China, strives for an 'authoritarian Internet' where surveillance and identification technologies help ensure social cohesion and security. The 'commercial Internet' desired by Washington DC sees online resources as private property, whose owners can monetise them and seek market rates for their use. Finally, certain states see the openness of the Internet as a vulnerability that can be

[113] K. Pistor, 'From Territorial Sovereignty to Monetary Sovereignty' (2017) 18(2) *Theoretical Inquiries in Law* 491, 496.

[114] K. O'Hara and W. Hall, 'Four Internets: The Geopolitics of Digital Governance' (CIGI Papers No. 206, December 2018).

[115] See Thornhill, above n 51.

exploited to further their geo-political projects. These four Internets (and the free rider) co-exist uneasily. We have not reached an equilibrium, and we need to be prepared for the Internet to evolve with the geopolitical ascendancy of one or another faction.[116]

These divergent visions reflect different responses to the 'convulsive rescaling' of our social and economic world and a redefinition of the relation between political economies and legal authorities. The so-called 'California Ideology' behind the Silicon Valley open Internet, for example, is (in broad terms) a product of the 'collision and synthesis' of neo-liberalism, counter-culture radicalism, and technological determinism.[117] Eclectic, it bears hallmarks of similarity to diverse conventional views, particularly Austrian School, free-banking, American Libertarianism, and the New Left. It combines a New Left anti-corporate ethos and faith in the Internet as a forum for new forms of community with a conservative libertarian faith in the ability of information technologies to facilitate voluntary exchange between individuals outside the sphere of state control.[118] Digital authoritarianism, on the other hand, is typified by robust assertions of national sovereignty over cyberspace that undermine the notion of cyberspace as a *situs* of international information flows and as a domain of individual privacy. It is illustrated in the 'Great Firewall of China'[119] as well as in efforts such as the Shanghai Cooperation Organisation through which China, Russia, India, Iran, and others have coordinated their Internet security policies to prevent the Internet being used as a site of political mobilisation against incumbent politico-legal structures.[120]

In a charming investigation from 2001, Viktor Mayer-Schönberger sets out an account of this problematic dramatized as a four-act play. His *dramatis personae* are 'Legal Authority' and 'Cyberspace'. The stage is spare. 'Act One: Collision Course' sees Legal Authority subjugating Cyberspace. 'Act Two: Almost Déjà Vu' sees the *arriviste* subjugating Legal Authority. 'Act Three: Separate Lives' sees the protagonists occupy a common stage but talking past each other without meaningful interaction. 'Act Four: Dialogue and Discourse' sees the characters learning to sing a common tune.[121] Along with one's assumptions about scale (ie where norms governing cyberspace ought to be promulgating and enforced), one's preferred mode of interaction shapes one's preferred regulatory landscape.

Outlook: the governance of cyberspace and Fintech regulation

It is not always straightforward to apply existing regulatory frameworks to new technologies;

[116] *ibid*, 13.

[117] R. Barbrook and A. Cameron, 'The California Ideology' (1995) 1(3) *Code*, http://www.metamute.org/editorial/articles/californian-ideology.

[118] See Lastra and Allen, above n 14, 16 and, by way of example, the reading list of the self-styled 'Satoshi Nakamoto Institute', URL: http://nakamotoinstitute.org/literature/.

[119] See eg Jyh-An Lee and Ching-Yi Liu, 'Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China' (2012) 13 *Minnesota Journal of Law, Science, and Technology* 125.

[120] See Liaropoulos, above n 52, 29.

[121] V. Mayer-Schönberger, 'The Authority of Law in Times of Cyberspace' (2001) 1 *Journal of Law, Technology & Policy* 1.

regulated activities are defined in legal instruments that typically predate the technologies driving the Fintech revolution, and some of these instruments have strong path-dependency effects that potentially make regulation by analogic application sub-optimal. Although principles-based regulatory frameworks can be flexible and *prima facie* technology neutral, Julia Black has observed, following their failure in the GFC, that such frameworks are subject to confounding factors including problems of interpretation, communication, compliance, enforcement, internal management, ethics, and trust.[122] Indeed, principles-based regulation may not be as technology-neutral as intended; it may presuppose categories of object and action that do not capture innovations fully.[123] As Reed observes, 'technology neutrality' means a number of different things.[124] Truly technology-neutral drafting is no mean feat, and it is sometimes better to draft laws to be technology-*specific* until the potential uses of the technology mature.[125]

The crux of the problem of Fintech regulation is the relation between the *conceptual* notion of risk management and the *institutional* dimension of 'market regulation' or 'state intervention' in financial applications of novel technology.[126] This relation is informed not only by the geopolitical state of play, but also the shape of the market, for example the current dominance of Internet-based platform providers. The global community struggles within the Westphalian paradigm to govern use of the atmosphere, the poles, or the high seas, or to tackle pandemic disease —despite unprecedented international cooperation in all of these areas in the decades since WWII. Moreover, the position of the nation state *vis-à-vis* private associations and business organisations has changed dramatically in the past decades; European capital markets and corporate governance regulation, for example, were described by Zambunsen in 2009 as a 'semi-autonomous', transnational legal field that incorporated 'hard' and 'soft' law norms promulgated by a 'panoply of public and private actors'.[127] What Josh Fairfield observes of gaming communities might pertain to financial services, too: 'It seems unlikely that real-world nations will recognise online communities as separate and co-equal sovereigns', he says, '[b]ut it is likely that real-world courts will seriously consider the norms generated by online communities as courts take up the task of applying law to virtual worlds.'[128] While we do not believe that the Internet will or should spell the death of the Westphalian nation state,[129] we

[122] J. Black, 'Forms and Paradoxes of Principles Based Regulation' (2008) 3(4) *Capital Markets Law Journal* 425.

[123] See eg, Rogers, above n 68, 690; J.G. Allen, 'Negotiability in Digital Environments' (2019) 34(7) *Butterworths Journal of International Banking and Financial Law* 459.

[124] See generally Reed, above n 6.

[125] Reed, above n 10, 201, 202.

[126] This is paraphrased from P. Zambunsen, 'The Next "Great Transformation" of Markets and States in the Transnational Space: Global Assemblages of Corporate Governance & Financial Market Regulation' (2009) 5(2) *Comparative Research in Law & Political Economy*, 4, in turn citing Saskia Sassen, *Territory—Authority—Rights: From Medieval to Global Assemblages* (Princeton University Press 2006).

[127] *ibid*, 14.

[128] Fairfield, above n 53, 831.

[129] See Zekoll, above n 82, 345, 349.

expect—and welcome—both cooperation between nation states and hybrid public/private norm-creation in response to financial stability risks originating in cyberspace.

With the benefit of these insights, we now make a few observations on the regulation of Fintech.

First, the regulation of Fintech would appear to be another chapter in a much larger struggle by the nation state, as one form of geo-political ordering, for regulatory primacy over transnational actors and economic processes that unfold within and beyond the borders it projects.[130] In the context of finance, this struggle has often been catalysed by new technologies. Thus, as novel as any financial technology is, it is important to remember that many of these questions have arisen before.

Secondly, an effective regulatory regime for Fintech might not resemble the ideal type of financial regulation in previous decades. As Zambunsen observed of the GFC, the globalisation of corporate activity and finance worked against attempts to 're-domesticate' corporate governance into the contained political economies of nation-states. He argued instead for a 'transnational' corporate governance regulatory framework[131] embracing regional and international legal harmonization and regulatory cooperation, soft law such as standards, industry self-regulation, and other hybrid forms of norm-creation and enforcement. Two sub-points follow from this. First, the difficulty of policing the third border speaks to regional and international cooperation. The expansion of harmonised 'law spaces', and the increased cooperation between local regulators that this implies, effectively reduces the number of territorial jurisdictions and the number of divergent rule-sets between them. By cooperating, states can prevent a race to the bottom and ensure that those posing a systemic risk to any financial system can be effectively regulated. Secondly, we think that national regulators should be open to the idea of working through self-regulatory efforts in cyberspace. This does not mean that cyberspace should be recognised as a jurisdiction in its own right. But where actors are willing to establish zones of legality in cyberspace, national regulators should work with rather than against them. These two processes could be mutually complementary: self-regulation could occur under the aegis of existing international cooperation that can claim an element of international legal authority.[132]

Financial globalization has been fostered not only by financial innovation and the technological revolution but also by the integration and liberalisation of markets and the mobility of people and capital. This calls into question the primacy that national regulators continue to place on national borders (what we have referred to in this article as the second border). It also calls into question the evolution of the global financial market, which is not homogenous but resembles a radial web with multiple interconnections and linkages, in which a few players dominate the

[130] Zambunsen, above n 126, 18.

[131] *ibid*, 23.

[132] Much of the early debate between 'cyber-separatists' and 'cyber-nationalists' was at cross purposes: see Fairfield, above n 52, 829.

scene. The dichotomy between global finance and domestic financial regulation, which features prominently in the work of Emilios Avgouleas, Douglas Arner, and Rosa Lastra[133] has given rise to the predominance of soft law and soft power, in the absence of 'hard' international financial law and 'formal' international financial regulators (with the IMF and the BIS having a limited mandate in this regard). The reliance on soft law and soft power,[134] highlights the complexities of regulating Fintech, but also points to a potential solution. Soft law is law, after all, and fills a vacuum. Indeed, the role of soft law instruments in internet financial governance ought to be further developed as part of a new 'financial *lex cryptographica*', including 'top-down' rules or principles (standards issued by intergovernmental or official entities), 'bottom-up' rules issued by private actors, associations and market entities (uniform rules and standards, voluntary codes of conduct, codes of practice, etc) which are also an exercise in self-regulation, and rules 'encoded' in Fintech systems themselves.[135]

Thirdly, territorial sovereigns retain leverage over those acting in cyberspace to the extent that human beings must live somewhere. Actions in cyberspace that are outright illegal, ie fraudulent or dishonest, can be more easily enforced when the human actors behind the scheme have lives and assets in the jurisdiction. It is not always straightforward to connect an individual in physical space to actions in cyberspace, just as it is possible (without the use of Fintech) to obfuscate the link between a taxpayer and their wealth through the interpolation of companies and trusts, for example. But most innovators are implicated in the conventional legal and financial system and this renders some of the cyber-sovereignty rhetoric otiose. We would also add that, although we have used cryptoassets as an example in this article, that focus can give a false impression. Most Fintech start-ups are conventionally 'rational actors' and often *seek* regulation. Indeed, the long-term challenge may come from large technology firms engaging in financial services, rather than techno-libertarian start-ups. The larger challenge in the long term can be seen if we look to recent developments in China, where telecommunications and e-commerce giants have established financial services ecosystems, replete with an established, captive user base. Facebook's Libra proposal provides another example on the horizon.[136] Long term, these concerns may be more challenging for the existing financial regulatory system than coalitions of banks and start-up technology partners.[137]

---

[133] See E. Avgouleas, *Governance of Global Financial Markets, the Law, the Economics, the Politics* (Cambridge University Press, 2012); E. Avgouleas, R.P. Buckley and D.W. Arner, *Reconceptualising Global Finance and its Regulation* (Cambridge University Press 2016); R.M Lastra, Inaugural Lecture at Queen Mary University of London (23 March 2011), URL: https://www.qmul.ac.uk/law/media/law/docs/podcasts/lastra2011_transcript.pdf; Lastra, above n 28, ch 14.

[134] C. Brummer, *Soft Law and the Global Financial System: Rule Making in the 21st Century* (Cambridge University Press 2011), ch 3.

[135] See Lastra, above n 28, ch 14; M. Giovanoli, 'A New Architecture for the Global Financial Markets: Legal Aspects of International Financial Standard Setting' in M. Giovanoli (ed), *International Monetary Law. Issues for the New Millenium* (Oxford University Press, 2000), 10 and n 25; De Filippi and Wright, above n 11, 5-7.

[136] See Libra Association Members, above n 15.

[137] This point was made by Adrian Blundell-Wignall during a panel discussion at IWFSAS (Cass Business School London, 11 September 2018).

Fourthly, to the extent that the physical layers of cyberspace rest in a jurisdiction, the entities that operate its infrastructure (eg, Internet service providers) can be co-opted into the regulatory framework.[138] There are limits to the extent to which regulators can legitimately require intermediaries to enforce their rules in cyberspace;[139] this is, in our view, one of the main contexts in which different visions of the Internet will compete. Contributions to the normative debate about the proper degree of openness in the context of consumer protection and systemic risk will be important in the coming years.

Fifthly, regulators may need to use enhanced technology to govern cyberspace. Most innovation in regulation and supervision technology (so-called 'Regtech' and 'Suptech') to date has occurred on the side of regulated or supervised entities, rather than regulators or supervisors—in particular, tools for digitising compliance and reporting processes to increase efficiency.[140] We would echo calls for an approach combining data, digital identity, and regulation that goes beyond digitising analogue-era processes and exploring the affordances of novel ICT for regulators.[141] In a sense, the emerging 'financial *lex cryptographica*' might contain technically-encoded norms that are intended to enforce state regulation rather than displace it. One approach might be an extension of 'sandboxes'[142] beyond temporary testing environments to permanent sites within cyberspace, provided by territorial sovereigns, from which Fintech providers can access nationally regulated financial markets—subject to built-in (automated) monitoring and control. This could comprise an element of both territorial and personal jurisdiction (or their analogues).[143]

CONCLUSION

This article has presented an extended borders metaphor, teasing out what is meant by 'regulated' and 'unregulated', examining the notion of territorial jurisdiction, and exploring the ontology of cyberspace in order to understand how current innovations might challenge financial regulation practically and conceptually. In particular, we have considered whether it is worthwhile to think expressly in terms of a third border between the 'real world' financial system and 'cyberspace'. The ultimate question is always whether a certain action is regulated in a jurisdiction. However, it is in our view worthwhile to introduce a third border into the

[138] See J. Black 'Enrolling actors in regulatory systems: examples from UK financial services regulation' [2003] *Public Law* 63.

[139] See eg *Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (2011) Case C-70/10.

[140] As regards 'Suptech' see https://www.bis.org/fsi/publ/insights9.pdf and https://www.esma.europa.eu/press-news/esma-news/regtech-and-suptech-–-change-markets-and-regulators.

[141] Arner, Barberis and Buckley, above n 3.

[142] See eg Financial Conduct Authority, 'Regulatory sandbox' (November 2015), https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf.

[143] Territorial insofar as a regulator creates a 'space' with infrastructure to connect to the regulated financial system, and personal to the extent that entry might work on an 'e-residency' basis for enterprises who wish to enter the space, irrespective of their real-world residency. See eg, the Estonian e-residency programme: https://e-resident.gov.ee/.

model. The first border highlights the challenges posed by *unregulated entities* engaging in *regulated activities* (or regulated entities engaging in unregulated activities) whether within a jurisdiction or across jurisdictions; the second border highlights the challenges posed by entities transacting across jurisdictions in ways that potentially circumvent or undermine national financial regulations; and what we have identified as a the third border usefully highlights the challenges posed by entities that either intentionally use the Internet to avoid national regulations, or use it to deliver financial services in ways that makes regulation practically or conceptually difficult.

This extended borders metaphor provided a perspective from which to consider current debates about the role of nation states in governing Internet-based activities that may not take place (straightforwardly) within their jurisdiction, but which might affect their national financial and economic system. The map is not the territory, and the utility of a model is ultimately assessed by reference to its explanatory purpose.[144] For the purpose of charting the future course of the emerging 'financial *lex cryptographica*' and conceptualising its relation to national law, we think that the perspective provided by the borders metaphor is useful. Though it was beyond our present ambitions to present a complete theory of Internet jurisdiction, we hope that our contribution to the ontology of cyberspace in the context of financial services has helped to shed some light on the 'digital real'. The result is a more nuanced vision of both domains, with a third border holding heuristic value but not necessarily reflecting intuitive notions about the digital *versus* physical phenomena. This, we hope, will help to anchor the notion of financial stability in a proper jurisprudential groundwork for further development as new challenges arise for national regulators.

We are still some way off a non-controversial theory of how computer networks that represent 'domains' of interaction fit within the conventional system of territorial sovereignty. It seems fair to say that some of cyberspace's properties would be lost from view if we simply reduced it to its physical layer. Likewise, to treat cyberspace as a full-blown territory would seem to make too much of what is, at base, a sound metaphor—but still a metaphor. There are competing values at stake, including the need to foster beneficial innovation and preserve the Internet as a free space for human interaction, that demand special consideration. We accept—as we assume most scholars of law and finance would—the value of a free and internationally open Internet, provided certain conditions are met. Both over-heavy governance of the Internet by states and an overly *laissez-faire* approach by nation states could lead to problems—the former to Balkanisation behind national firewalls[145] (likely with thriving black markets), and the latter to a 'Wild West' in which important public interests such as consumer protection and financial stability are neglected.

We may thus have to change the way we conceptualise and enforce jurisdiction as more of our social reality moves online. The future of cyberspace governance is, for now, open; in our view,

[144] A. Korzybski, *Science and Sanity: An Introduction to Non-Aristotelian Systems and General Semantics* (The International Non-Aristotelian Library Publishing Co 1933), 58.

[145] See Liaropoulos, above n 52, 29.

Fintech will continue to provide an important context for mapping its borders. Our preferred outcome is Mayer-Schönberger's Act Four, and our predisposition is towards Brussels' 'bourgeois Internet'. Sovereign states still have a unique and irreplaceable role that must be reflected in the emerging law of Internet jurisdiction. But, we think, there is a place for both supra-national cooperation and user-generated ordering in the Internet. In terms of the former, we would especially stress harmonisation at the European level. We would also stress the role of standards and other 'soft law' instruments. In terms of the latter, we remain open to the role of private and quasi-public actors in Internet governance, particularly in the formation of soft law instruments.

Wherever the next systemic shockwaves are going to originate, we would close with the same warning Goodhart and Lastra made in 2010. Regulation usually follows crises counter-cyclically. While it is undesirable to stifle innovation, it is even less desirable to allow systemic risks to proliferate below the radar and to act only once they eventuate.