BORDER PROBLEMS II: MAPPING THE THIRD BORDER

JASON G ALLEN AND ROSA M LASTRA

[2018] *UNSWLRS* 88

UNSW Law
UNSW Sydney NSW 2052 Australia

Border Problems II: Mapping the Third Border

J.G. Allen and R.M. Lastra*

Abstract

In the last 20 years, the Internet has become the site of economically and legally relevant objects, events, and actions. It has also become the source of potential risks to the financial system. Building on one of the authors' prior work on 'border problems' in financial regulation, in this contribution we concretise what is meant by 'regulated activities' and 'regulated entities' by reference to the logic of deontic modes implicit in the concept of regulation (in the most common, narrow sense of being prohibited without a positive permission, and being permitted on terms including ongoing supervision). We also explore the way that technology makes new forms of action possible, which the law must then regulate, whether through the application of existing norms or the promulgation of new ones. We then move to examine what is meant (and assumed) by 'territorial jurisdiction', a difficult concept that is often used but not always properly understood. This provides an entry point into a conceptual exploration of a third border, that between the 'real world' (which we take to mean conventional social, legal, and economic reality) and 'cyberspace' as a domain of human interaction that is facilitated and conditioned by digital communications systems. Accepting the metaphor of place-ness implicit within the notion of cyberspace, we offer some ontological observations on the nature of both the 'real world' and 'cyberspace' with an eye towards locating, raising, and policing the boundary. Surveying the greatly divergent approaches currently taken to borders in cyberspace, including 'Californian techno-liberalism' and 'Chinese digital authoritarianism', we advocate a 'third way' which accords both states and other stakeholders (including private actors) a role in the governance of cyberspace. However, based on our understanding of financial stability and systemic risk, we argue that conventional sovereign states have a unique and irreplaceable role that must be reflected in the emerging law of Internet jurisdiction. We conclude with a few

* J.G. Allen is an Alexander von Humboldt Foundation Post-Doctoral Fellow at the HU Berlin *Großbritannien-Zentrum*, a Visiting Fellow at the UNSW Faculty of Law and an Adjunct Research Fellow at the University of Tasmania Faculty of Law.

Professor Rosa M. Lastra is the Sir John Lubbock Chair in Banking Law at the Centre for Commercial Law Studies, Queen Mary University of London.

An early version of this paper was presented at the Sheffield Institute for Corporate and Commercial Law 4th Law and Money Conference on Banking in the Shadows – FinTech, Cryptocurrencies and Emerging Financial Systems (University of Sheffield, 3 September 2018). Parts were also presented at the International Workshop on Financial System Architecture and Stability 2018 (Cass Business School, 10-11 September 2018) and at the LSE Systemic Risk Centre conference on The Future of Money and the Impact of Fintech and Cryptocurrencies (LSE London, 26 November 2018). The authors would like to thank the organisers and participants of these events for their valuable feedback. The authors would also like to thank Ross Buckley, Anton Didenko and Charles Goodhart. The usual disclaimer applies—all errors remain our own. All URLs last accessed 21 November 2018.

more concrete observations on what all this could mean for financial regulation in the coming decade.

1. Introduction

Following the 2008 Global Financial Crisis ('GFC'), C.A.E. Goodhart and R.M. Lastra presented a 'border problems' metaphor to highlight two basic tensions in the regulation of financial markets. They explored two borders: (i) the border between regulated and unregulated entities and (ii) the border between national jurisdictions.[1] As we explain below, when these borders are crossed, the regulated (national) economy faces risks originating in unregulated spaces, with potential implications for both consumer protection and financial stability.

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 other places. Since the 1990s, cyberspace has become the *situs* of economically important—and therefore *prima facie* legally relevant[2]—objects, events, and actions.[3] Currently, innovations in financial technology ('Fintech') are making the Internet an important channel for the delivery of financial services and products.[4] Fintech-driven financial services are diverse, including finance and investment (e.g. crowdfunding and P2P lending), payments, money, exchanges and infrastructure (e.g. mobile money, virtual currencies including 'cryptocurrencies', and foreign exchange), and consumer interface (e.g. mobile application-based financial services).[5] Many of these operate in the 'shadow' industry, i.e. in parallel to conventional, regulated firms. Although Fintech-based financial products and services are subject to existing regulations, and although principles-based regulations are capable of applying to novel socio-technological practices, *prima facie*, the growth of Fintech could cause border problems because it (i) delivers new financial products and services that have not yet been regulated (e.g. 'cryptocurrencies' or 'crypto assets' generally), (ii) utilizes new forms of business organization that are not necessarily recognized by the legal system (e.g. 'distributed autonomous organisations'), and (iii) operates in a 'space' which is, by nature, non-territorial or difficult to define in terms of territorial jurisdiction (i.e. 'cyberspace').

The premise of this paper is that to understand the potential risks posed by Internet-based

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

[2] See J.G. Allen, 'Property in Digital Coins' (2019) *European Property Law Journal* (forthcoming).

[3] We take 'actions' to be a sub-category of 'events' which are the consequence of an intentional dealing by an entity recognised to be a legal subject. In the near future, cyberspace could well become the *situs* of new kinds of legally relevant *actors*, as well, but the entry of legally cognizable non-human agents raises a whole raft of complex issues which we are unable to deal with in this paper.

[4] See D.W. Arner, J.P. 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.

[5] 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.

financial services, it is helpful to understand the notion of 'cyberspace' itself. As the term itself implies, cyberspace is the communications within a network of digital computers *conceptualised as a place*. In a seminal (if now dated[6]) article, for example, D.R. Johnson and D.G. 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.'[7] Inherent in the idea of cyberspace is a metaphor; 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.[8]

In this paper, we consider whether it is appropriate to incorporate this notion of 'place-ness' by adding a third border to the border problems metaphor to understand the potential impact of Fintech on conventional financial regulation. Assuming that it is, we offer some analysis of the nature of cyberspace with particular reference to financial services and the regulatory objective of financial stability. While the concept of financial stability has become 'mainstream' in the decade since the GFC, in our view it has yet to be sufficiently anchored in conventional legal and jurisprudential basis. In particular, given the transnational nature of systemic risks generally, the nature of financial stability interacts awkwardly with the notion of national territorial jurisdiction—especially in the context of Internet-based financial services.

This paper is structured as follows. Section 2 elaborates what the borders are and why they are important. Section 3 then concretises the 'known' borders, highlighting the relevant features that we think will help us to understand the posited third border. In particular, we set out what we understand by 'regulated activities', 'regulated entities', and 'territorial jurisdiction'. Section 4 sets out our conception of 'cyberspace'. Section 5 explores how the border between 'cyberspace' and the 'real world' operates conceptually, and how it might be guarded. We conclude with some recommendations and questions for further research in Section 6.

---

[6] D.R. Johnson and D.G. Post, 'Law and Borders—The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1367. One of the more dated claims in the paper is the claim that 'No one accidentally strays across the border into Cyberspace', and that 'Crossing into Cyberspace is a meaningful act that would make application of a distinct "law of Cyberspace" fair to those who pass over the electronic boundary.' (at 1379). Even accepting this controversial proposition *arguendo*, its premise is no longer factually true—the online and offline worlds are increasingly seamless, and we frequently stray online without being fully aware of it, or even find records of events and actions (i.e. photographs) 'popping up' in places we did not mean to put them. In the future, it will probably become even more difficult to tell when we are using 'just' a computer and when we are using a computer connected to the Internet. In the financial context, the use of intermediaries (who use the Internet) makes this claim even more problematic—why should territorial sovereigns with a consumer protection and financial stability mandate (for example) entrust intermediaries to design and promulgate rules of the space in which those intermediaries act for their principals?

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

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

2. 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 regulation that bites penalises those within the regulated space, relative to those just outside the regulated space, causing substitution flows towards the unregulated space.[9] 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.[10]

To use an imperfect but useful metaphor, the topography of markets is such that, like water, financial activity flows downhill and around high points. This was illustrated in 2008 by commercial banks opening up associated conduits, structured investment vehicles, and hedge funds, which contributed to the GFC. This pressure has perhaps increased with the increased burden of compliance following the crisis, and the means of border crossing have potentially increased. And, like territorial waters in international maritime law, borders are often the source of conflicts.

As an example of the pressure behind substitution flows, R.M. Lastra and J.G. Allen's recent analysis for the European Parliament ECON Committee 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, which operate in parallel to regulated financial services. The sale of 'equity' type tokens in so-called Initial Coin Offerings ('ICOs') as a substitute for sale of company shares to conventional venture capital investors has seen a massive flow of capital into early stage ventures, many of which effectively circumvented capital markets and consumer protection requirements such as prospectus disclosure and corporate governance (e.g. listing) standards that would otherwise have applied. Crypto-based financial services are also frequently concentrated in permissive jurisdictions, from where they aim to service consumers in more strictly regulated markets.[11] Although we concluded that the overall size of the 'crypto' market is probably not yet systemic, there are significant incentives for institutional money to flow into the new crypto-token based financial

[9] C.A.E. Goodhart, 'The Boundary Problem in Financial Regulation' (2008) 206 *National Institute Economic Review* 48.

[10] C.A.E. Goodhart and R.M. Lastra, 'Border Problems' (2010) 13(3) *Journal of International Economic Law* 705, 706.

[11] 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 Ruth 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.

economy, and we recommended that regulators remain vigilant.[12] Another example comes from the rise in peer-to-peer lending and other 'informal' financial arrangements in China. As Fabio Braggion, Alberto Manconi, and Haikun 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.[13]

2.1. Relation Between the Borders

It is also convenient to consider, as a preliminary matter, how our borders relate to each other conceptually. As our analysis unfolds, it will become clear that, in a certain sense, the second border is just an outgrowth of the first. Financial regulation ultimately takes place on a national level, but financial activity is transnational, so national financial systems are inherently vulnerable to the effect of actions taken outside the jurisdiction.[14] Entities that are unregulated because they are foreign, for example, are at base just a category of unregulated entities—an entity regulated in Jurisdiction A is 'unregulated' in Jurisdiction B. 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.

In a similar manner, the third border may just be 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 borders metaphor, i.e. by allowing us to isolate the relevant issues of national jurisdiction *versus* international financial transactions, we think it is worthwhile to explore a third border to highlight the relevant issues faced when conventional regulators attempt to govern objects, events, and actions in cyberspace. Chief among these issues 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 D.W. Arner, J.N. Barberis, and R.P. Buckley call 'FinTech 3.0'. FinTech 2.0, they explain, continued until the late 2000s and was characterised by things like Bankers' Automated Clearing Services ('BACS'), Clearing House Information Systems ('CHIS'), and Society of Worldwide Financial Communications ('SWIFT'). FinTech 3.0 is marked by ICT such as distributed ledger technology ('DLT'), but also by changed business models and players—not only start-ups but also technology and

[12] R.M. Lastra and Jason 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).

[13] Fabio Braggion, Alberto Manconi and Haikun 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.

[14] The case of supranational regulations, such as those found in the European Union, do not change this basic fact; supranational regulations are still supra*national*, deriving ultimately from national sovereignty and governing an area ultimately defined by national borders. However, as we explain below, supranational regulation is better equipped to regulate transnational commerce because it casts a broader net.

telecommunications companies entering into the financial services sector.[15] As we explain in more detail below, there is some overlap between FinTech 2.0 and FinTech 3.0, as the later stages of the former utilised Internet-based ICT. But Fintech 3.0 is characterised by novel objects and modes of action (such as crypto-tokens, cloud-based computing, and DLT) and by the agency of non-traditional intermediaries (and attempts to disintermediate and/or automate intermediation). This, in our view, raises some challenges for conventional regulation which is based on (i) paper-based objects, (ii) centralised actors (especially intermediaries), and (iii) centralised information repositories.

Mapping the border between the 'real world' and 'cyberspace' is especially difficult 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 account legally for what Tom Boellstorff calls the 'digital real'.[16] The effort is worthwhile because armed with such an understanding, we can respond more intelligently and pro-actively to new forms of financial activity in the coming decades.

3. The Known Borders

The two borders discussed by Goodhart and Lastra are familiar terrain; lawyers are used to (i) categorising the world of possible objects, events, and actions as 'regulated' and 'unregulated', and (ii) to carving the world up into so many 'jurisdictions', i.e. spheres in which legal rules apply or have force. Yet, despite the familiarity, concretising what we mean by 'regulated activity', 'regulated entity', and 'national jurisdiction' is an essential first step.

3.1. Regulated Activities and Entities

What does it mean to say that something is 'regulated' or 'unregulated'? There are a few ambiguities in the way this term is used which are easily dealt with, but can get in the way if left unnoticed. It is helpful to separate regulated *activities* from regulated *entities* and to discuss them separately.

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

[15] FinTech 1.0, they argue, began with early telecommunications cables in the mid-19th century and ended with early digitalisation in the 1960s; 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, 8, 12, 20. Much of the current banking system still relies on essentially Fintech 1.0 infrastructure.

[16] See Tom Boellstorff, 'For Whom the Ontology Turns: Theorizing the Digital Real' (2016) 57(4) *Current Anthropology* 387.

prohibited, and possibly sometimes *obligatory*, but neither prohibited nor obligatory in all cases.[17]

It is a truism that everything which is not prohibited is permitted. Generally, it is also accurate to say that the default mode in a free market economic order (certainly in the Anglo-American world) is permissive rather than prohibitive—that I am allowed to do any action not expressly or implicitly prohibited. However, due to the potentially harmful or repugnant nature of some activities, the default mode is prohibition. In such cases, a positive permission ('license') is required, which is generally granted on terms. So, for example, driving is an activity that is generally prohibited except for licensed drivers, and those drivers are subject to numerous regulations. Lending to consumers is another. This is often, but not always, what is meant by 'regulated' in the financial services context.[18] To be more precise, 'entities licensed to do something *prima facie* prohibited' is usually what we mean by 'regulated entities', and '*prima facie* prohibited activity permissible with a license' is usually what is meant when we speak of 'regulated activities'. Less often, but also frequently, we use 'regulated activities' to refer to activities that are not subject to a licensing (positive permission) regime, but which are subject to oversight and/or intervention by some authority if the bounds of the regulated are transgressed.

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*. There was no point in saying that flying was regulated, for example, until manned 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. 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. The significance of this will appear when we come to explore cyberspace as a *situs* of actions that are not possible in the physical world. We posit the advent of Internet-based financial record-keeping and transacting as an extension of a deep pattern in the history of finance, namely of new technologies (whether the printing press or DLT) enabling new forms of market activity to which the law must respond.

What emerges, then, is a more complex proposition. We are concerned with actions that have two axes: in this logic, an action can and must be described as both (i) permitted/prohibited/obligatory *and* (ii) possible/impossible/necessary. These two axes set a

[17] Modal logic is the branch of formal logic that extends propositional and predicate logic to modality, i.e. the feature of language that communicates qualifications about a proposition that need not be actual. For an explanation that covers both modal logic and deontic logic, see James Garson, 'Modal Logic' in E.N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2016 Edition), https://plato.stanford.edu/archives/spr2016/entries/logic-modal/.

[18] There are some activities that have no licensing requirement as such but are subject to oversight and regulation—take for example the private placement of securities. In this sense, (almost) all activities are 'regulated', which is probably why the term is usually used in the narrower sense of 'licensable'. The terms licence, charter, authorisation (associated with the 'entry into the business' of commercial banks) 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'.

'liberty-space' (i.e. set of actions the actor is *permitted* to do) and an 'ability-space' (i.e. set of actions the actor is *able* to do). These together form a 'possibility-space'[19]—one axis being 'deontic', i.e. that 'action *x* is permitted/prohibited/obligatory for agent *y*' and one axis being 'capacitative', i.e. 'action *x* is possible/impossible/necessary for agent *y*'. It is the conjunction of these two axes that is most important: actions that are *possible* and *prohibited* (or *conditionally permitted*, which is also to say *conditionally prohibited*) are the most interesting to lawyers, as this is where the wheels of the law start turning; actions that are *impossible* but *permitted*, for example, are not very interesting in a practical legal sense. The interesting part of the border, then, is between actions that are made possible by new technology to which the law has taken a prohibitive or conditionally permissive stance.

Moving on, what does it mean for an *entity*, as distinct from an *activity*, to be 'regulated'? In usage, it is usually the positive permission sense of 'regulated' that is intended. Saying that an entity is regulated is more likely to imply that the activity in question has been deemed to be *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 ordinary persons may not. Every regulated entity, therefore, has a unique possibility-space composed of its ability-space and liberty-space, the latter of which will generally be hedged by conditions including ongoing procedural conditions such as record-keeping and reporting.

The deontic axis of a regulated entity's *Spielraum* is likely to be the focus of attention, as business corporations are usually taken to have the capacity to perform all actions. However, at other times, for example under the 19th century doctrine of corporate *ultra vires*, asking whether a company had acted as permitted was a second step; it was first necessary to ask whether the company had *validly performed any action at all*. Although we are unused to stating explicitly that different classes of agent exist, with different ability-spaces,[20] thinking in such terms is important for lawyers to 'interface' with the rule-based universes of cyberspace. The concept of 'space' is used differently in law, physics, mathematics, and philosophy, but the use of a space or place-ness metaphor to describe the virtual realms of human interaction made possible by the Internet and other developments in ICT is an important point of articulation or even convergence between these disciplines.[21] This is important to keep in mind as we consider the future of financial regulation below. For example, DLT is being

[19] Lars Lindahl suggests *Spielraum*, i.e. 'play space' by analogy with the established *Entscheidungsraum*, i.e. 'decision space': see Lars Lindahl, 'Hohfeld relations and *spielraum* for action' (2006) 26(2) *Análisis Filosófico Online*, http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1851-96362006000200007. The regulatory sandbox approach recommended by the UK Financial Conduct Authority and other regulators to foster innovation reminds us of this 'play space'. See https://www.fca.org.uk/firms/regulatory-sandbox

[20] We have probably forgotten this point in our effort to leave the bad old days of institutionalized discrimination behind. For example, in the 19th century, English law limited the range of possible actions that women were able to perform. For example, one case held: 'Generally speaking, a married woman cannot execute a deed; she can do no act of this description, except in respect of an estate settled to her separate use, or in the exercise of a power given to her.' *Whitmarsh v Robertson* (1845) 1 Coll 571, 575. If a married woman attempted to execute a deed (in the absence of such a power), she did not act in a manner beyond the scope of her *permission*; she acted in a manner beyond the scope of her *legal ability*.

[21] See for example the introduction given in Binxing Fang, *Cyberspace Sovereignty: Reflections on building a community of common future in cyberspace* (Springer 2018), 12.

used to create so-called 'decentralised autonomous organisations' ('DAOs'), which some claim to be business organisations without human organs. It will be necessary in the future to decide what, if any, legally cognisable ability-space such an entity ought to have within a (nationally) regulated market space. It may also be desirable or even necessary to limit the kind of actions entities are capable of performing, such that their ability-space matches their liberty-space. We see this as a potentially exciting area of development for 'regulatory technology' ('Regtech').

3.2. Territorial Jurisdiction

Broadly stated, a jurisdiction (from Latin 'law' and 'speaking') is a context in which the authority of some legal institution applies. Jurisdiction becomes important when parties transact economically 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. For our purposes, the crucial thing about the concept of jurisdiction is that each jurisdiction makes a limited claim to its rule-set's validity—it does not generally posit a general rule-set for all actions by all actors in all places, but a limited rule-set for certain actions (and possibly certain actors) in certain places. The aspect on which we wish to focus in our paper is captured well by the German term *Geltungsbereich*—that is the area in which laws *gelten*, which means to be valid and in force (we lack a direct cognate in English).[22] So, for example, I can say (i) that drinking beer under the age of 21 is prohibited in the United States, and (ii) that drinking beer after age 16 is permitted in Germany without contradiction, because these norms have different *Geltungsbereiche*.[23]

Indeed, because rule-sets are made by communities of human beings, many legal systems operate with some notion of *personal* jurisdiction.[24] In such a system, the context in which a rule-set applies is social, e.g. derived by ancestry or religion or voluntary oath of allegiance. But, perhaps because human communities occupy physical space, and often claim exclusive law-making power over the space they occupy, modern conceptions of jurisdiction often assume 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.[25] Systems of purely personal jurisdiction are rare; more common are spheres of personal jurisdiction under

[22] See Eugenio Bulygin, 'Valid Law and Law in Force' in Eugenio Bulygin (Carlos Bernal *et al* eds.), *Essays in Legal Philosophy* (Oxford 2015), 285.

[23] Some states assert extra-territorial *Geltungsbereiche* for their norms. For example, some states extend norms against the consumption of other drugs to citizens worldwide, thus asserting a personal jurisdiction outside the territory: 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.

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

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

the aegis of a territorial sovereign, such was the status of Jews in the Holy Roman Empire or under Ottoman *millet* system.[26]

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 organization 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.[27] Intuitively, when we think of jurisdiction today we tend to think of states, i.e. we take territorial jurisdiction for granted. Further, for largely historical reasons, the state seems like an inevitable, even natural category in jurisprudence, and the deontic incidents of 'state status' seem like inevitable outgrowths of it. 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.

Because of this, we tend to think of territorial jurisdictions as geographical entities that belong to the 'real world' or, as Johnson and Post put it, the 'world of atoms'.[28] Of course, this is not really true; the territory is just a set of arbitrary geographical coordinates,[29] and the state is no more a given feature of the 'world of atoms' than a centimetre or a country club.[30] There is nothing about the left bank of the river Rhine that makes it French and there is nothing about the right bank that makes it German; these are social impositions on the natural world.

The ontic furniture[31] of our world sometimes makes more sense if we start with less grandiose examples than the Westphalian nation state. We therefore take two examples of jurisdiction writ small to illustrate our point.[32] First, let us consider an *eruv*—an urban area demarcated

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

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

[28] D.R. Johnson and David Post, 'Law and Borders—The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1367, 1368

[29] See generally Barry 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).

[30] On the ontology of the state, see e.g. David Tan, 'The Metaphysics of Statehood' (2018) 31(2) *Canadian Journal of Law & Jurisprudence* 403. See also Joseph Raz, 'Why the State' and Detlef von Daniels, 'A Genealogical Perspective on Pluralist Jurisprudence' in Nicole Roughan and Andrew Halpin (eds.), *In Pursuit of Pluralist Jurisprudence* (Cambridge 2017), Chapter 7 and Chapter 8 respectively.

[31] The term is take from Uskali Mäki, 'Scientific realism as a challenge to economics (and vice versa)' (2011) 18(1) *Journal of Economic Methodology* 1, 8; see also Uskali Mäki, 'Scientific Realism and some Peculiarities of Economics' in R.S. Cohen, Risto Hilpinen, and Qui Renzong (eds), *Realism and Anti-Realism in the Philosophy of Science* (Kluwer 1996).

[32] Not only are these examples physically smaller than (most) states, but they are also examples only of a territorial parameter in which a rule-set is said to apply; they allow us to bracket out, for the time being, considerations of institutional competence etc and to focus on the *Geltungsbereich* as a legally-constituted social delimitation of physical space.

within a larger urban area by means of a boundary, usually marked by given landmarks such as telephone poles.[33] The purpose of an *eruv* is to turn an area halachically (i.e. according to Jewish law) into a 'private' domain, instead of a 'public' one, such that certain prohibitions (e.g. of carrying objects outside the private domain on *Shabbat*) do not apply. It is therefore an invisible border, defined by reference to landmarks, that has important deontic consequences, specifically enlarging the liberty-space those that create it such that certain general prohibitions do not apply. An *eruv* is quite specific to the community that creates it; different *eruvim* in the same city maintained by different Jewish communities may intersect and overlap. Communities from different parts of the world that follow the same tradition may adopt each other's *eruvim*, but communities from the same city that follow different traditions may not regard each other's' *eruvim* as kosher.[34] Secondly, let us consider the *cippi* stones of the *pomerium* of ancient Rome. This line was originally (probably) a defensive wall, but by classical times it had already come to assume primarily 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 the example of a prohibition on carrying, citizens were not allowed to bear arms within the *pomerium*.[35]

These two geographically-defined social spaces differ in important respects. An *eruv* is created and maintained by a small, specific religious community, while the *pomerium* was created by a large imperial power. *Eruvim* currently exist, whereas the *pomerium* is but no longer maintained by the collective beliefs or practices of any living community—to the extent it exists at all, it exists as a historical social fact. But both of these social spaces are community-specific, and neither of them are features of the 'real world'—at least not straightforwardly in the way that their markers (e.g. telephone poles and white stones) are features of the real world. True, they 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. But they fall

[33] Barry Smith explains that, to constitute an *eruv*, a given area of public space must be demarcated from its surroundings, either by wires or by some sort of wall or fence (or combination thereof), or by virtue of its topography (for example because it is all higher or lower than its surroundings). See Barry Smith, 'On Place and Space: The Ontology of the Eruv' in Christian Kanzian (ed.), *Cultures: Conflict—Analysis—Dialogue: Proceedings of the 29 International Ludwig Wittgenstein Symposium* (Ontos 2007), 403. Jewish law is delightfully pragmatic in how certain of its notorious strictures can be fulfilled; in 1992, one community submitted a planning application to erect metal poles with strands of nylon fishing line stretched between them at a height of 10 meters to construct an *eruv*. See also Michele Rapoport, 'Creating Place, Creating Community: The Intangible Boundaries of the Jewish "Eruv"' (2011) 29(5) *Environment and Planning D: Society and Space* 891; Barry Smith and Leo Zaibert, 'Real Estate: The Foundations of the Ontology of Property' in Heiner Stuckenschmidt, Erik Stubkjaer, and Christoph Schlieder (eds.), *The Ontology and Modelling of Real Estate Transactions* (Ashgate 2003).

[34] This lends some support to the notion of 'groupjectivity' presented in Raimo Tuomela, *Social Ontology: Collective Intentionality and Group Agents* (Oxford University Press 2013), 220.

[35] Julius Caeser thus had the *pomerium* to thank for meeting his demise on the Ides of March; on this day, the senate met in the extra-mural theatre instead of meeting in the intra-mural forum, such that the conspirators could avoid breaching the prohibition against carrying arms *intra muros*. See S.B. Platner (Thomas Ashby ed.), *A Topographical Dictionary of Ancient Rome* (Oxford 1929), '*pomerium*'.

squarely within the domain of social reality, not the world of atoms.[36]

The history of the concept of territorial sovereignty in the early modern period offers some important insights into the interplay between technology and socio-political practices. According to Jordan Branch, technological advances in the practice of cartography both pre-dated and causally influenced political and legal conceptions of sovereign space. He argues, by extensive reference to the historical sources, that mapping technology made the notion of absolute, homogenous sovereign territories with contiguous, non-overlapping borders possible before rulers actually started asserting the kind of territorial sovereignty typical of 'Westphalian' modernity.[37] Prior to this, sovereign territories were conceptualised and represented as non-contiguous 'islands' of authority based around important sites like towns and cities; overlapping zones were common in the penumbra of such political power centres. This is a reminder that we must be receptive to the way that new technologies not only undermine conventional perceptions of politico-legal authority, but also enable rulers to stake new claims and influence the kind of claims they are likely to make. As in the historical process of state-formation, the role of local and 'private' organisations within this newly-mapped landscape, in which interstitial spaces are eliminated, is a characteristic feature of cyberspace.[38]

Thus, as we discuss below, the developing notion of Internet governance and the agency of territorial sovereigns in cyberspace has the potential to reshape our basic conceptions about the way that human communities associate and govern their social lives. While in the early days of the internet this insight was often pushed to further a more or less radical libertarian project, we think it is important for more conventional legal analyses to take the challenge seriously and respond appropriately and in a timely fashion.

4. The Third Border: Cyberspace

As an environment framed by physical and non-physical components including a global network of digital computers, cyberspace poses an implicit challenge to the traditional idea of global governance that is mainly state-centric.[39] Perhaps for this reason, many classical (especially early) accounts of law in cyberspace characterized cyberspace as a realm completely apart from physical reality. For example, the thrust of Johnson and Post's argument was that cyberspace could not be governed effectively by the assertion of territorial jurisdiction over Internet-based information flows.[40] Their 'place-ness' argument served a

[36] See D.G. Post, 'How the Internet is making jurisdiction sexy (again)' (2017) 25 *International Journal of Law and Information Technology* 249, 250.

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

[38] See e.g. Elina 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.

[39] 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.

[40] See D.R. Johnson and D.G. Post, 'Law and Borders—The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1367, 1370-1378.

techno-libertarian normative project; they also argued that cyberspace would, and ought to be allowed to, create its own normative order(s), and that 'virtual jurisdictions' ought to be treated like territorial jurisdictions, i.e. in being allowed to create divergent rule-sets.[41] In general we are sceptical of this argument, at least in its more strident versions,[42] but we do agree with certain of their suggestions, for example of multilateral regulation of cyberspace, e.g. through global registration systems for domain names.[43] In our (more conventional) view, national 'law spaces' will remain important in the sphere of financial regulation, and this makes crucial to map the border between national 'law spaces' and 'cyberspace'.

Position in the contemporary debate about Internet jurisdiction have been categorised by A.N. Liaropoulos as falling into three main models: 'distributed governance', 'multilateral governance', and 'multi-stakeholderism'.[44] Each of these approaches offers different answers to the questions whether cyberspace should be governed at all and who should govern it (particularly, what role different actors including firms, non-governmental organisations, states, and supra-national organisations should play in that governance). Views range from out-and-out Internet anarchism to the complete subordination of the Internet to national jurisdiction through the creation of national Intranets. We are unable to offer a fully-developed theory of Internet jurisdiction here, nor are we able to present a developed normative argument for the approach that we prefer. It is sufficient to state that we take a broadly multi-lateral governance approach, in which conventional state sovereigns have a distinct and essential role to play, but in which a legitimate role exists for private and quasi-public actors, as well. Our main objective in this section is to present a set of methodological considerations that we think are essential to frame the debate—which we think will increase in intensity over the next decade—in the context of financial services.

The starting point, again, is how cyberspace is presented as a 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

[41] See D.R. Johnson and D.G. Post, 'Law and Borders—The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1367, 1387, 1400.

[42] See R.M. Lastra and J.G. Allen, 'Virtual Currencies in the Eurosystem: Challenges Ahead', a policy contribution 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), 15. See also Rheinhard 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; Andreas Manolopoulos, 'Raising "Cyber-Borders": The Interaction Between Law and Technology' (2003) 11(1) *International Journal of Law and Information Technology* 40; Lorna 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.

[43] D.R. Johnson and D.G. Post, 'Law and Borders—The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1367, 1380.

[44] 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), 27.

> 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.[45]

If they are correct, then those who advocate the regulation of financial markets by conventional territorial sovereigns must develop a sophisticated understanding of cyberspace as a place and articulate its connection to the conventional category of jurisdiction. Again, the most important thing to remember is that the border between cyberspace and the 'real world' is not a border between an informational domain and a physical domain; what we call the real world is not composed of rocks and trees but of invisible, legally-constituted objects. In one of the first concerted 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, either.[46] In particular, the ontological status of legal objects and entities has been largely ignored by analytical legal theory, and, despite a well-developed literature on deontic logic (e.g. W.N. Hohfeld's logic of jural relations and the secondary literature it has spawned), the logic of legal action has been relatively neglected, as well.[47] Yet, even while philosophers have not yet adequately addressed the ontological problems of cyberspace, lawyers have had to deal with the practical problems of computerised media. This leads to the counter-intuitive insight that an exploration of cyberspace might actually be able to teach us something about the ontology of the law.

The notion that cyberspace acquires 'place-ness' in virtue of the fact that messages accessed there are persistent over time, and are accessible to many people regardless of physical location, is a metaphor, but it holds an ounce of good sense: In our view, it mirrors the role of communications and documents in the constitution of our social world more broadly.[48] For example, how are territorial jurisdictions created (and changed)? The answer is through *speech-acts*, usually in documents—declarations of independence, constitutions, town charters, planning applications, religious documented utterances actually *constitute* the political geography of the world around us. Only in the second instance are physical things like walls and boundaries constructed to mark their borders.[49] In fact, most of law's stock-in-trade is

[45] D.R. Johnson and D.G. Post, 'Law and Borders—The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1367, 1378, 1379.

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

[47] See generally Lars Lindahl, *Position and Change* (Reidel 1977), 3, 193. See also Jennifer Frey, 'Analytic Philosophy of Action: A *Very* Brief History' (2013) 7 *Philosophical News*, https://www.philosophicalnews.com/wp-content/uploads/2017/07/7.5.pdf.

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

[49] For example, Plutarch records of what would become the *pomerium*: 'When Romulus was digging a trench where his city's wall was to run, Remus ridiculed some parts of the work, and obstructed others. At last, when he leaped across it, he was smitten (by Remus) and fell dead there.' (Plutarch, *Vitae Parallelae*, *Romulus*, 10, 1-2). Detlef von Daniels observes that what Remus failed to recognize was precisely the *normativity* the structure expressed: see Detlef von Daniels, 'Normativity and the Sources of International Law' in Samantha Besson und

invisible: you can't paint a right blue,[50] you can't pack it in a box, and it does not need refrigeration; a corporation has no body to kick and no soul to damn.[51] When a regime changes, many of these entities (from land titles to public debt instruments to units of money) *prima facie* disappear with it, subject to rules of state succession. How, then, do we know they actually exist?[52] The answer is that we *document* their existence with title deeds, lease agreements, memoranda of understanding, marriage certificates, brewing licenses, letters patent, degree certificates, debentures, certificates of incorporation, share certificates, acts of parliament, orders in council, judgments, affidavits, witness statements, tax assessments, and so forth. With these documents, we create vast and complex structures within institutional legal reality.[53] Barry Smith argues, in terms that mirror Johnson and Post's emphasis on endurance and self-identical replication:

> 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 (for example to form audit trials), 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, of claimant to adjudicator, of doctor to patient, and so on. 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. The effect is that private memory traces inside human brains are prosthetically augmented by publicly accessible documents and associated document technologies.[54]

These invisible objects, events, and actions structure our social lives. Ultimately, they help to structure the interactions between physical human bodies and physical objects in the world around. A significant part of our lives as human beings, however, 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.[55] A game of chess, for example, is much more than pushing

---

Jean d'Aspremont (eds.), *The Oxford Handbook on the Sources of International Law* (Oxford 2017).

[50] See Christian von Bar, *Gemeineuropäisches Sachenrecht* (Beck 2015), para [80].

[51] See John 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.

[52] In the story by Hans Christian Andersen, swindlers tell the emperor that they will make him the finest vestments that will be invisible by all those who are unworthy of their office or stupid; as a result, the emperor and all his courtiers pretend that they can see the clothes. Ultimately, a common child calls out that the emperor is not wearing any clothes at all. The story was reportedly inspired by Andersen's childhood memory of standing in a crowd to see King Frederik VI of Denmark. When the king appeared, young Andersen exclaimed: 'Oh, he's nothing more than a human being!' See Hans Christian Andersen (Vilhelm Pedersen and Lorenz Frølich eds.), *The Stories of Hans Christian Andersen* (Granta 2004), 267.

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

[54] Barry Smith, 'How to Do Things with Documents' (2012) 50 *Revisti di Estetica* 179, [11].

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

pieces around a wooden board; in virtue of rules, new forms of action become possible (such as 'taking a queen', 'being in check', 'cheating', and 'winning') that would simply make no sense without reference to the rules. Even if, ultimately, the *telos* of a financial capitalist economy is to feed, clothe, and shelter human bodies, the way in which it achieves these ends is more akin to a game of chess than farming (pushing counters around a *banco* or trading pieces of paper that embody abstract rights). And while a business firm might reduce, on one view, to a structure of human bodies working together to produce widgets, such a view ignores many of the most interesting features of a corporation.[56] Further, it does not explain the fact that financial firms produce not widgets, but rather new pieces and new moves in financial games.[57]

On the view we have adopted, institutional objects, events, and actions are created (mainly) through declarative speech acts. In hyper-literate societies like our own, most of these speech-acts come to take written form, and then to form Smith's 'document complexes'. Although a part of institutional legal reality is not constructed in writing, the lion's share of it is. The point we seek to establish is that the 'real world' (let alone the 'world of atoms') is a misleading way of talking about conventional legal, political, and economic reality. The border between territorial jurisdictions and cyberspace is a border between different sub-domains of technologically-mediated social reality—not one between the physical world and a technologically-mediated domain of social reality. On one side is a sub-domain housed largely in paper, and on the other a sub-domain housed largely in computer systems (of different kinds). We either need to erect an artificial border, between, for example, electronic bank deposits and bitcoins, or we need to accept that much of our conventional economic reality is already located in cyberspace, and that the main difference between cyberspace and conventional legal reality is in the kind of documentary medium used to create and manipulate objects.

What we are witnessing now is a rapid expansion in the complexity of documentary complexes 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) has made new types of 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.[58] True, there may be ontologically relevant differences between paper-based and digital documentary complexes;[59] we can anchor paper-housed legal objects in the 'real world' in virtue of their physical embodiment, and we can place digitally-housed legal objects in

[56] See Simon Deakin, 'Tony Lawson's Theory of the Corporation: Towards a Social Ontology of Law' (2017) 41 *Cambridge Journal of Economics* 1505.

[57] For an extended analogy between chess and money, which is quite common in the social ontology literature on money, see Ingvar Johannson, 'Money and Fictions' in Felix Larsson (ed.), *Kapten Nemos Kolumbarium* (Göteborg University 2005).

[58] See e.g. Mareille Hildebrandt, 'Law *as* Information in the Era of Data-Driven Agency' (2016) 79(1) *The Modern Law Review* 1, 1.

[59] 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.

'cyberspace' because they exist in a different medium. But it is also important to recognise that they both belong to a single domain of social reality ('legal reality') that is mediated and facilitated by information technology. It is also important to remember that, for all the novelty of DLT (for example), communities often place economic importance on a new class of intangible artefact, and the law usually limps along behind—but eventually catches up. The history of finance is full of examples, but think only of the history of the joint stock corporation and its shares a.k.a. 'equity capital' which were not recognised by the common law courts.[60]

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 now DLT attenuate the link between geography and institutional legal reality quite radically. The latter seems to be cut loose, floating in parallel to conventional institutional legal reality. Because of the nature of the ICT on which it rests, this (sub-domain of) reality is, in principle, accessible by everyone at all times irrespective of their geographical location (or the jurisdiction in which that geographical location lies). Restrictions on access are not based on geographical location but on rules, whether privately or publicly promulgated. Of course, there are physical barriers to access: more than a billion people live behind a state-imposed firewall,[61] and the billions lack access to the internet for want of a connection, an Internet-capable device, or electricity to charge it.[62] But these do not negate the 'place-ness' of cyberspace as posited by Johnson and Post. For the purposes of national regulators responsible for overseeing transactions in financial instruments—rights 'enclosed in a paper'[63] or housed in a computer server—the existence of a de-territorialised cyberspace poses both conceptual and practical problems.

5. Guarding the Third Border

How, then, do we guard the third border? Cyberspace, we have argued, provides a *situs* for objects, events, and actions that are given relevance in the domain of social reality we have called *legal institutional reality*. When one transfers demand deposits in an account held in one's name with a commercial bank to an account in another name with a commercial bank, 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 yet done a very good job of mapping this familiar terrain; international private law, for example, raises questions such as 'Where is a

[60] See Paddy 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.

[61] See e.g. 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.

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

[63] See e.g. Arianna Pretto-Sakmann, *Boundaries of Personal Property: Shares and Sub-Shares* (Bloomsbury 2005), 73-74.

bank account?'[64] or 'Where is a debt?',[65] but has not provided very compelling answers; we rather tend to avoid such questions wherever possible.

First it is necessary to note that cyberspace would be irrelevant if the objects, events, and actions in it were not given relevance by the relevant legal system. For example, dealing with *World of War Craft* 'gold' in a game account is not to same as dealing with US dollars in a bank account, just as taking of *Monopoly* money (within the context of game-play, at least), is not the same as taking real cash. A dollar of book money (demand deposits), a bitcoin, and a 'coin' *World of Warcraft* gold are the same in many technical respects: their data structure and the manner of storage may differ, but they are all constructed purely of data. The difference is that our legal system positions demand deposits differently, i.e. imposes a different status on them, even though *World of Warcraft* 'coins' are of value to some people, and markets exist for them in the 'real world'.[66] The law takes cognizance of the *World of Warcraft* coin more mediately, i.e. as a set of obligations governed by the game's end user license agreement ('EULA'). Although the 'EULA' governing my relationship with my bank does not impress upon 'my' demand deposits the status of 'property' straightforwardly, the suite of legal protections is more extensive and robust to ensure standards of conduct from commercial banks and to protect demand deposits in virtue of their monetary status.[67]

When we speak of cyberspace in the context of the shadow financial system, we are speaking of objects, events, and actions in cyberspace which are *prima facie* legally cognisable, e.g. obligations that articulate with the 'real world' in a manner qualitatively different to *World of Warcraft* gold. This seems to be a fact-driven phenomenon, i.e. the law often follows the market in this context; when (enough) market participants start attributing 'real world' value to outlandish cyber-objects, the border is crossed. When the border is crossed such that events in cyberspace can destabilise the 'real world' economy, it is *prima facie* a matter of interest to regulators. For example, where a regulated financial entity has taken a position in 'crypto assets' such that it would suffer liquidity problems if the USD:BTC exchange rate shifted, the border is crossed—even though the national regulators may not have taken an official stance

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

[65] P.G. Rogerson, 'The *Situs* of Debts in the Conflict of Laws: Illogical, Unnecessary and Misleading' (1990) 49 *Cambridge Law Journal* 441.

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

[67] Compare Financial Conduct Authority, 'Unauthorised payments from your account' (13.01.2018), https://www.fca.org.uk/consumers/unauthorised-payments-account; see the thread at https://www.wowhead.com/forums&topic=218841. See generally F.G. Lastowka and Dan Hunter, 'The Laws of the Virtual Worlds' (2004) 92(1) *California Law Review* 1, 29, 40; J.J. Kayser, 'The New New-World: Virtual Property and the End User License Agreement' (2006) 27 *Loyola of Los Angeles Entertainment Law Review* 59; S.H. Abramovitch and D.L. Cummings, 'Virtual Property, Real Law: The Regulation of Property in Video Games' [2007] *Canadian Journal of Law and Technology* 73; Ronan Kennedy, 'Virtual rights? Property in online game objects and characters' (2008) 17(2*) Information & Communications Technology Law* 95; C.J. Cifrino, 'Virtual Property, Virtual Rights: Why Contract Law, Not Property Law, Must be the Governing Paradigm in the Law of Virtual Worlds' (2014) 55(1) *Boston College Law Review* 235; James Bonar-Bridges, 'Comment: Regulating Virtual Property with EULAs' (2016) *Wisconsin Law Review Forward* 79, http://wisconsinlawreview.org/comment-regulating-virtual-property-with-eulas/.

on Bitcoin. 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), the major challenges of the market in 'crypto-currencies' and the Fintech revolution more broadly.

As noticed above, it would be possible to collapse all three borders conceptually into one, i.e. 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 digital tokens, for example: the US Securities Exchange Commission ('SEC') has taken a pro-active stance by treating many ICOs as the issue of securities (despite their issuers' attempt to avoid engaging in a regulated activity at all)[68] and the US Commodities Futures Trading Commission treating certain 'crypto-tokens' as commodities.[69] In general, however, it is not always straightforward to apply existing regulatory frameworks to new technologies; 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.[70] Although principles-based regulatory frameworks can be flexible and *prima facie* technology neutral, Julia Black has observed (following their failure in the GFC) that they are subject to confounding factors including problems of interpretation, communication, compliance, enforcement, internal management, ethics, and trust.[71] In our view, one major issue is that even principles-based regulations may not be as technology-neutral as commonly assumed; they too often presuppose categories of object and action that may not capture innovations optimally.[72] For example, regulators around the world are currently scrambling to define digital tokens, and problems arise both at the level of describing tokens as objects of property rights, and at the level of describing tokens as units of money, securities, commodities, contracts for futures, etc. Although a novel object can be shoehorned into an existing category, the path-dependencies inherent in each jurisdiction's legal system can lead to irrational national divergences that could, in turn, increase jurisdictional arbitrage—and therefore pressure on the third border.

---

[68] See e.g. 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.

[69] See e.g. *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.

[70] For example, it would appear that some crypto-assets are intended to be 'digital bearer instruments', in which property is (i) conceptually possible and (ii) passes with 'possession', but the law of negotiable instruments logically presupposes a physical (paper) instrument.

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

[72] See e.g. 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.

5.1. The Empire Strikes Back?

D.G. Post has observed, in a more recent contribution, that apparently 'territory-defying' technologies are, paradoxically, making jurisdiction even more important. The possibility of action at a distance, and the 'convulsive rescaling' of our social and economic world it causes, not only challenge the conventional framework of territorial jurisdiction but also underscore the importance of geo-political power in our (ultimately physical) world. Although he and many others thought that national boundaries were about to disappear in the 1990s, Post reflects, 'it appears now that more resources than ever are being diverted to shoring them up.'[73] 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. As C.S. Maier observes the importance of the third border in the grand sweep of modern history:

> The result [of the spread of these new technologies] transform[s] 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.[74]

The Internet jurisdiction debate takes on particular nuances in the context of financial services delivery and regulation. Maier's division is reflected, for example, in the contrast between 'Californian techno-liberalism' and 'Chinese digital authoritarianism'.[75] The so-called 'California Ideology' is eclectic; in broad terms, it is a product of the 'collision and synthesis' of neo-liberalism, counter-culture radicalism, and technological determinism that 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.[76] Needless to say, the libertarian strand of this movement is inimical both to conventional regulatory institutions and structures at both the national and supra-national level.[77] Because of its eclecticism, it bears hallmarks of similarity to diverse conventional views, particularly Austrian School, free-banking, American Libertarianism, and the New Left. Digital authoritarianism, on the other hand, is typified by robust assertions of national sovereignty over cyberspace that not only

[73] See D.G. Post, 'How the Internet is making jurisdiction sexy (again)' (2017) 25 *International Journal of Law and Information Technology* 249, 253, 255.

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

[75] See John Thornhill, 'There is a "third way" for Europe to navigate the digital world' (*Financial Times*, 20 November 2018).

[76] Richard Barbrook and Andy Cameron, 'The California Ideology' (1995) 1(3) *Code*, http://www.metamute.org/editorial/articles/californian-ideology. An idea of the literature influential on this demographic is gleaned from the reading list of the self-styled 'Satoshi Nakamoto Institute': See http://nakamotoinstitute.org/literature/.

[77] See R.M. Lastra and J.G. Allen, 'Virtual Currencies in the Eurosystem: Challenges Ahead', a policy contribution 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).

undermine the notion of cyberspace as a *situs* of international information flows but also as a domain in which individuals have some legitimate private sphere. It is illustrated in the 'Great Firewall of China'[78] as well as in efforts such as the Shanghai Cooperation Organisation through which China, Russia, India, Iran, and certain Central Asian states have coordinated their Internet security policies to prevent the Internet being used as a site of political mobilisation against incumbent politico-legal structures.[79]

In our view, Internet jurisdiction is a conversation that is about to begin in earnest.[80] And it is worth noting that the current position of the debate—and the state of Internet-based finance and commerce—is dominated by players based in jurisdictions that tend towards one or the other of the above-named poles. John Thornhill, characterising President Emmanuel Macron's case for a better regulated and democratic internet as an enlightened way to tackle 'surveillance capitalism and a social media cacophony', has advocated a European approach—a 'third way' between Californian libertarianism and Chinese authoritarianism—as a better way to strike a deal between the need to protect citizens and foster innovation, so as 'to deploy technology for the public good'.[81] Such a third way, we think, would accord a place for both robust national financial regulation and non-state-based ordering in the Internet. In terms of the former, we would especially stress the importance of harmonisation at the European level, as well as international cooperation and standard-setting more broadly. In terms of the latter, we remain open to the role of private and quasi-public actors in Internet governance, and accept the *prima facie* value of a free (and international) Internet, provided certain conditions are met. Both over-heavy governance of the Internet by states and an overly *laissez faire* approach by states could lead to problems—the former to a 'Balkanisation' of cyberspace behind national firewalls[82] (likely with a thriving black market circumventing them), and the latter to a 'Wild West' in which important public interests such as consumer protection and financial stability are neglected. Thus, while treating cyberspace as a jurisdiction tantamount to a foreign state would concede the point too easily, we may have to change the way we conceptualise and enforce jurisdiction as more of our social reality moves online. We therefore assume that there is a third border, and that it is worthwhile and legitimate for conventional sovereigns to enforce that border to an appropriate extent. What remains is to determine that extent and to anchor it in a coherent concept of jurisdiction that applies both to the conventional social world and to cyberspace.

[78] See e.g. 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.

[79] See 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), 29.

[80] See D.G. Post, 'How the Internet is making jurisdiction sexy (again)' (2017) 25 *International Journal of Law and Information Technology* 249, 257-258.

[81] John Thornhill, 'There is a "third way" for Europe to navigate the digital world' (*Financial Times*, 20 November 2018).

[82] See 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), 29.

5.2. Borders to What End?

In our view, the objectives of consumer protection and financial stability help to frame, and thus delimit, that extent. The concept of financial stability has gained in relevance in recent years—it was somewhat 'rediscovered' or 'revamped' following the GFC. But, as a goal, it is difficult to define and is more identifiable in its negative definition (i.e. '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'.

Financial stability complicates the border problems because it transcends institutional mandates[83] and geographical boundaries. Financial stability is indeed a national, regional and international goal; episodes of instability, like a tsunami, do not respect territorial boundaries. George Sheldon and Martin Maurer put the point evocatively:

> 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.[84]

Indeed, systemic risk ('contagion risk') in a general sense is a phenomenon not confined to economics or to the financial system. For instance, consider health: throughout history there have epidemic diseases (the Great Plague in the Middle Ages, the Spanish Flu after World War I) where widespread contagion crossed jurisdictions with devastating effect. Systemic risk in financial markets has been defined as the risk that financial difficulties at one institution or more spill over to a large number of other institutions or the financial system as a whole.[85] While some identify this risk with default or credit risk, in our opinion any risk—including liquidity risk, interest rate risk, exchange rate risk, or any of the risks associated with Fintech and the growth of 'crypto' assets—can grow to systemic proportions when its negative impact extends beyond an individual institution and affects or threatens to affect other institutions. When this occurs, it often creates a disruption in the financial and payments systems and even the economy at large.

Systemically Important Financial Institutions ('SIFIs') are institutions that are so important for the functioning of the financial system that their problems—and, in particular, their failure—

[83] In the US, the 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 principle federal financial regulators (replacing the President's Working Group on Financial Markets) Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203 (2010). The Act, named after Senator Christopher Dodd and Congressman Barney Frank, was signed by President Obama on 21 July 2010.

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

[85] Davis defines 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. See Philip Davis, *Debt, Financial Fragility and Systemic Risk*, (Oxford: Clarendon Press, 1992), 117.

can trigger systemic risk.[86] SIFIs present additional challenges to the delimitation of borders because the Internet offers unparalleled opportunities for circumventing ('gaming') financial regulations such as those identifying and controlling SIFIs.[87] As Goodhard and Lastra observed in their previous investigation of 'border problems':

> 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 TBTF, 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. Does it follow then that regulation thereby enhances the dangers of systemic collapse that its purpose should be to prevent? Does the desire to encourage all the regulated to adopt, and to harmonize on, the behaviour of the 'best' actually endanger the resilience of the system as a whole?[88]

The definition of a systemically significant financial institution is also dynamic: what is systemic today is not necessarily what will be systemic in future. Indeed, this is where the borders of the Fintech and crypto-space become so relevant. 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. However, again, cooperation between states logically presupposes and practically relies on national territorial jurisdiction.

5.3. Raising borders in cyberspace[89]

Legal systems take a variety of approaches to establishing jurisdiction in cases where jurisdiction is disputed, for example where the matter of a transaction or an action has a connection with more than one jurisdiction. Each legal system's choice of law rules, for example, determine the proper law of a contract or a tort by reference to the nationality and

[86] See e.g. the so-called 'Geneva Report' by Brunnermeier, Marcus Andrew Crocket, Charles Goodhart, Avinaush Persaud and Hyun Shin, "The Fundamental Principles of Financial Regulation", *Geneva Report on the World Economy* (February 2009). See also C.A.E. Goodhart and R.M. Lastra, 'Border Problems' (2010) 13(3) *Journal of International Economic Law* 705.

[87] See C.A.E. Goodhart, "Problems of Monetary Management: The U.K. Experience" in Anthony S. Courakis (ed.), *Inflation, Depression, and Economic Policy in the West* (Rowman & Littlefield 1981), 111.

[88] See Goodhart and Lastra, 'Border Problems' (2010) 13(3) *Journal of International Economic Law* 705, 712-713.

[89] This turn of phrase is taken from Andreas Manolopoulos, 'Raising "Cyber-Borders": The Interaction Between Law and Technology' (2003) 11(1) *International Journal of Law and Technology* 40.

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 and before the advent of modern ICT, i.e. in the pre-Fintech, Fintech 1.0 and early Fintech 2.0 periods, and, while they provide an important part of the picture, they do not always apply straightforwardly to novel ICT.[90] For example, the idea that a bank account has a *situs* was difficult enough in the era of paper book-keeping; as J.H. Sommer has observed.[91] Things have only gotten more complicated with the advent of cloud computing and DLT, two of the most important technologies behind current Fintech innovations. Indeed, if we review the range of solutions in the conventional law, we will find that there is no 'silver bullet'[92] that will solve the jurisdictional problem; a combination of approaches is necessary, which may evolve over time.

First and foremost, it is necessary to distinguish between the various 'layers' of cyberspace, which are often neglected in legal analysis. Yochai Benkler has observed that there are three layers: (i) a *physical* layer (i.e. undersea cables, computer servers, and wireless routers), (ii) a *logical* layer (i.e. the rules governing access to and use of the network) and (iii) a *content* layer (i.e. the content actually being communicated, such as the data packet that constitutes a US dollar or a bitcoin).[93] We would add that a fourth layer—a *social* layer—sits on top of these technological layers, positioning banking records as 'real' assets and World of Warcraft gold as 'game' assets, making cyberspace a socio-technical system.[94] The concept of jurisdiction would seem to comprise part of this fourth layer. Likewise, the concept of jurisdiction, argues Geist, comprises three layers: (i) the courts (and other legal institutions) that could have jurisdiction, (ii) the substantive law that they would apply, and (iii) the enforcement of rulings based on that law in an online environment.[95] The technological layers of cyberspace relate to territorial jurisdiction in different ways. The physical layer is most easily brought under territorial jurisdiction; for example, fibre-optic cables will be physically located in a jurisdiction or, if under the sea outside of national jurisdiction, will belong to an entity that is a government or is the subject of a government. 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

[90] See Campbell 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, discussing the interaction of 19th century conflicts rules with cross-border communications systems, but also underlining the contribution of traditional international private law analysis, in the context of intellectual property law.

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

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

[93] 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.

[94] See e.g. Robert Cooper and Michael 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.

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

the content is accessible by (or targeted towards) users resident in another state, leading to a conflicts-type problem. Our application of regulations to Internet-based financial services, then, should not only be informed by an awareness of the layers involved in any given case, but also the aspects of jurisdiction that are being conceptually extended to cover the respective layers of the Internet.

Further, while a conflicts approach has the virtue of 'lowering the stakes' by allowing the courts of one state to assume jurisdiction but apply the norms of another state more appropriate to the matter,[96] a conflicts analysis alone will not get us home. D.J.B. Svantesson rightly argues that it is necessary to embrace not only conventional conflicts considerations, but international public law considerations, as well—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.[97] Combining these insights, it would seem to us that a proper approach requires a granular view of cyberspace *per se* (i.e. 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 states, and (iii) balances between these legitimate interests. In the context of financial regulation, we think that states' interests must centre on (i) consumer protection and (ii) promoting financial stability and resilience.

The task ahead is to develop a complete and coherent theory of Internet jurisdiction that rests on a proper understanding of where 'cyberspace' and the 'world of atoms' touch. Ultimately, the realm(s) of cyberspace reduce to electrons in a silicone microprocessor. The third border, then, is perhaps where a bitcoin sits on a miner's server, where an electronic funds transfer instruction travels through a fibre optic cable, and where a private key is kept in the memory of a human being who lives, breathes, and sleeps in a certain physical place. But we are still some way off a non-controversial theory of how all this works within the conventional system of territorial sovereignty—just as we are struggling to govern use of the atmosphere, the poles, pandemic disease, and the high seas within the 'Westphalian' paradigm (despite unprecedented international cooperation in the decades since the Second World War), we will likely struggle for some time to govern financial risks that move frictionlessly through national jurisdictions on the 'information superhighway'. 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' and helped to anchor the notion of financial stability in a proper jurisprudential groundwork.

6. Conclusion

[96] Campbell 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, 439.

[97] D.J.B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford 2017), Chapter 3.

In this paper, we have examined what is meant by 'regulated' and 'unregulated', examined the nature of territorial jurisdiction, and explored the ontology of 'cyberspace' in order to understand how current innovations in Fintech might challenge financial regulation in both a practical and a conceptual sense. In particular, we have explored whether it is worthwhile to think expressly in terms of a third border between the 'real world' financial system and 'cyberspace'. Our contribution is envisaged less as a direct substantive contribution to the emerging law of Internet jurisdiction, and more as a contribution to the ontology of the subject-matter illustrated with some reflections on the regulation of cross-border financial services.

Our analysis suggests that the third border is, at base, an aspect of the second, which is in turn an aspect of the first: ultimately, the basic question is whether an action is regulated in a jurisdiction and according to its rules. This, in turn, entails a proposition about the action being prohibited, permitted, or obligatory, which implies that the action is possible or necessary (but not impossible). However, it is in our view worthwhile to introduce a third border into the model, because each highlights unique difficulties: 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; the third border highlights the challenges posed by entities that either intentionally use the Internet to avoid national regulations completely, or use it to deliver financial services in ways that makes regulations practically or conceptually more difficult. The map is, to use a familiar dichotomy, not the territory, and the utility of a model is ultimately assessed by reference to its explanatory purpose.[98]

Thought it was beyond our present ambitions to present a mature theory of Internet jurisdiction, we hope that our ontological exploration of cyberspace might prove useful in this endeavour. In conclusion, we wish to make a few observations on the regulation of financial objects, events, and activities, in cyberspace.

First, the difficulty of policing the third border speaks, in our view, to regional and international cooperation. The expansion of harmonised 'law spaces', and the increased cooperation between local regulators that this implies, will 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 the financial system can be effectively held to account.

Secondly, territorial sovereigns still have considerable leverage over those operating in cyberspace because cyberspace rests ultimately upon physical layers: techno-libertarians have to live somewhere, and most of them appear to like living in Western liberal democracies that

[98] Alfred Korzybski, *Science and Sanity: An Introduction to Non-Aristotelian Systems and General Semantics* (The International Non-Aristotelian Library Publishing Co 1933), 58: 'A map *is not* the territory it represents, but, if correct, it has a *similar structure* to the territory, which accounts for its usefulness.'

respect their property rights. Actions in cyberspace that are outright illegal, i.e. fraudulent or dishonest, can be more easily enforced when the human actors behind the scheme have lives and assets in the jurisdiction. Further, the more physical and logical layers of cyberspace in a jurisdiction (or in another jurisdiction such as a Member State of the European Union with harmonised institutions, law, and enforcement), the more easily it can be regulated cyberspace. Again, this physical infrastructure has to be somewhere, and unless shadow financial services providers wish to move everything but the content layer of their cyber-services to a jurisdiction that has raced to the bottom, they will have to maintain some presence in the territory such that laws can be made to bite.

Thirdly, one of the difficulties of policing transactions in cyberspace is that the relevant actors are identities, like email addresses and usernames, rather than physical beings. Bitcoins, for example, are held pseudonymously, such that it is difficult to know who is actually transacting, with predictable consequences for financial crime, anti-money laundering, and counter-terrorism law enforcement. Although bitcoins present an unusual case, Fintech generally works with identities that may or may not be closely associated with 'real world' legal personalities. It is essential that national (and supranational) regulators insist on maintaining the link between the basic actor—the human being—and the online identity that transacts in cyberspace. The link between human beings and legal actors is notoriously tenuous already; complex webs of corporations, trusts, and other denizens of legal reality clog the efforts of tax authorities, for example, and a whole offshore economy thrives on 'gaming' the legal system.[99]

Fourthly, national regulators should be open to the idea of working together with self-regulatory efforts in cyberspace. We do not wish to concede too much on this point to arguments, such as Johnson and Post's early one, that cyberspace should be recognised as a jurisdiction in its own right. But where actors are willing to establish zones of legality in cyberspace—and, we would stress, to 'plug in' to national jurisdiction (for example for content targeted at some nationally regulated financial system)—national regulators should work with rather than against them. This could occur, for example, under the aegis of existing international co-operations that can claim an element of international legal authority.

Fifthly, national regulation may need to 'fight fire with fire' by using technology to monitor cyberspace. Most 'Regtech' innovation to date has occurred on the side of regulated entities, rather than regulators—in particular, we have seen innovation in tools for digitizing compliance and reporting processes to increase efficiency. D.W. Arner, J.N. Barberis, and R.P. Buckley argue for a reconceptualization of financial regulation towards an approach combining data, digital identity, and regulation that goes beyond digitising analogue-era processes and

[99] This is particularly important because, in the near future it will not only be humans and corporations that are performing economically and legally relevant actions in cyberspace—as machine learning and artificial intelligence advances, algorithms will become a more important class of actors and for the purposes of attribution it may be necessary to grapple with 'e-Persons' of different kinds. See Gerhard Wagner, 'Robot Liability' (June 19, 2018). Available at SSRN: https://ssrn.com/abstract=3198764.

exploring the affordances of novel ICT for regulators as well.[100] In our view, one approach to guarding the third border might be an extension of 'sandboxes'[101] 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 (and possibly automated) monitoring and control (and make financial cyberspace a hostile place from which to operate). This would consist in an element of both territorial and personal jurisdiction (or their analogues)—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.[102]

In the meantime, risks that enter at the retail or consumer side should be countered with warnings, education, and other such tools. Regulators are often powerless to stop individuals accessing unregulated financial services on their own initiative. But individual exposure of this sort is unlikely to present a danger of systemic risk. Systemic risks are much more likely to arise from regulated entities exposing themselves (for example a bank lending money to retail customers who then purchase digital tokens). Here we can observe parallels to the days before the GFC, as regulated entities engaged in business with novel financial instruments such as collateralised debt obligations. Over the coming decades, it is likely that we will see an increasing partnership between conventional banks and Fintech start-ups as technology partners, and this could cause 'border problems' in the short to medium term. On the up side, however, regulators have better prospects, all things being equal, of preventing licensed entities from engaging in risky activities, and, through pro-active regulation, this kind of risk could be kept in check. Although we have used digital tokens as an example in this paper, an undue focus on the 'crypto movement' can give a false impression. Most Fintech start-ups are more conventionally 'rational' and often seek regulation themselves. Indeed, the long-term challenge may come from large technology firms engaging in financial services, rather than Fintech start-ups. The larger challenge in the long term can be seen if we look to current developments in China, where telecommunications and e-commerce giants have established massive shadow financial services ecosystems, replete with an established, captive user base. Long term, it is likely that these concerns will be less invested in the existing financial regulatory system than a coalition of banks and their start-up technology partners.[103]

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. But, while it is undesirable to stifle beneficial innovation, it is even less desirable to

[100] D.W. Arner, J.N. Barberis, and R.P. Buckley, 'FinTech, RegTech, and the Reconceptualisation of Financial Regulation' (2016) 37(3) *Northwestern University Journal of International Law and Business* 371.

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

[102] See e.g. the Estonian e-residency programme: https://e-resident.gov.ee/.

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

allow systemic risks to proliferate below the regulatory radar and to act only once they eventuate. Regulation should occur pro-cyclically, which means pro-actively.