DIGITAL TECHNOLOGY-BASED SOLUTIONS FOR ENHANCED EFFECTIVENESS OF SECURED TRANSACTIONS LAW: THE ROAD TO PERFECTION?

TERESA RODRÍGUEZ DE LAS HERAS BALLELL[*]

I
INTRODUCTION:
A SECOND GENERATION OF DIGITAL LAW[**]

Digital technology has pervaded our society. It has penetrated markets, institutions, transactions, social relations, cultural, political, and educational environments. It exerts an extraordinary transformative force on structures, relations, and processes. At its initial stage of evolution, however, digital technology has been incorporated and understood as a mere instrument replacing other traditional media and means. Data messages, the digital medium, and electronic communications have been perceived and utilized as helpful and effective enablers of communication, content creation, and transactions management. Most legislation on electronic commerce, digital signatures, and information society services—employing the European Union legal terminology—views technology as a tool. Existing rules represent a laudable effort to legally recognize technology-mediated situations on the basis of functional equivalence and medium neutrality principles. The United Nations Commission on International Trade Law (UNCITRAL) adopted instruments on electronic commerce and electronic signature,[1] and their transpositions (or influence) in domestic and regional texts, constitute the fundamental pillars of

This article is also available at http://lcp.law.duke.edu/.

[*] Chair of Excellence at the University of Oxford (Commercial Law Center, Harris Manchester College) in the framework of the *UC3M-Santander Chair of Excellence program*, reciprocal with Professor Louise Gullifer (University of Oxford) at the Universidad Carlos III de Madrid. The author would like to acknowledge Universidad Carlos III of Madrid and Santander Bank for the granting of the Chair of Excellence, and the Harris Manchester College for the warm reception.

[**] Research Project *Reform of Spanish Laws of Security Rights in an international context* (DER2016-77695-P).

1. U.N. COMMISSION ON INT'L TRADE L. [UNCITRAL], UNCITRAL MODEL L. ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT, U.N. Sales No. E.99.V.4 (1996) [hereinafter UNCITRAL MLEC]; UNCITRAL, UNCITRAL MODEL L. ON ELECTRONIC SIGNATURES WITH GUIDE TO ENACTMENT, U.N. Sales No. E.02.V.8 (2001) [hereinafter UNCITRAL MLES]; UNCITRAL, U.N. CONVENTION ON THE USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS, U.N. Sales No. E.07.V.2 (2005) [hereinafter UNCITRAL CEC].

this first generation of digital law. These rules seek to create a common legal infrastructure for the negotiation, the conclusion, and to a certain extent—where the digital fulfillment is feasible, for instance, in case of digital assets, service provision, or electronic payments—the performance of contracts of almost any nature.

Nonetheless, that initial legal approach to digital technology has proven to be nearsighted. The acceleration and accumulation of technological developments pose unforeseen challenges to the twenty-first century's law. A systematic, extensive, and wisely combined application of these (no longer) emerging technologies, such as Artificial-Intelligence (AI), Internet-of-Things (IoT), and blockchain, offers fascinating possibilities and announces great disruptive effects, as witnessed with the development of smart property, smart contracts, new electronic platforms. Their expected repercussions on the legal system are immense, but are not yet fully understood. These technologies are poised to impact the core of private autonomy and its limits, the concept of a contract and its interpretation, the equilibrium of parties' interests, the structure and means of enforcement, the efficacy of legal and contractual remedies, and the vital attributes of the legal system of effectiveness, fairness, impartiality, and predictability. Technology repairs imperfections, enhances effectiveness, reduces costs, increases predictability, and provides celerity. It might be argued that these disruptive technologies prepare the law for a road to perfection. Or, maybe, they are paving the path towards a replacement of the law by technology.[2]

Such a defiant panorama requires serious reflection to define all the angles of the challenge, assess the likely consequences, and devise possible legal responses. Whereas the implications of the first-wave technology are successfully dealt with by the existing global legal framework for the use of electronic communications in business transactions, the right response to the second wave of technology developments must be carefully considered and mindfully implemented. Several responses are possible. First, a wait-to-see approach that inhibits any regulatory action until a total consolidation of technology advances and a full comprehension of their outcomes may be attractive. Second, continuity with the current approach may be the preferred route. This would imply reliance on the ability of existing technology-neutral rules to embrace any new development under a functional-equivalence basis. Therefore, no specific regulatory action would be needed. Third, an active response aimed to formulate specific legal rules for all or some technology developments could be chosen. Such a legislative option should articulate a previously well-defined set of policy issues determining whether the aim of those bespoke rules should be to enable, to ban, to limit, or simply to legally recognize the development and application of the target

2. Joel R. Reidenberg, *Lex informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) (coining, for the first time, the idea of *Lex Informatica)*. *See generally* LAWRENCE LESSIG, THE CODE IS LAW AND OTHER LAWS OF CYBERSPACE *(*1999). The second edition in 2006 was entitled CODE 2.0. The work was then reformulated and popularized by Lessig as "The Code is Law," even if the author nuanced the broad interpretation of that suggestive statement.

technologies.

The legal system surrounding secured transactions provides an exceptional context to frame the above-outlined debate, to test the application of described digital-technology solutions, to analyze their implications, and, therefore, to assess whether a specific legal response is required. In modern credit-based economies, secured transactions play a critical role. A sound, effective, and predictable secured transactions system repairs credit market failures and, accordingly, facilitates access to finance in competitive conditions. Therefore, all efforts made to enhance the effectiveness of the secured transactions system will directly benefit access to credit in today's economies. Access to credit, in turn, is a key driver for job creation, innovation, social inclusion, and economic growth. Hence, the secured transactions system is a strategic component of international trade and domestic economies. Nonetheless, the secured transactions system is imperfect too: publicity is limited, monitoring is costly, and enforcement is not fully effective.[3] The application of technology solutions could attenuate imperfections, repair failures, and enhance effectiveness of the secured transactions legal system. Insofar as reforms of secured transactions laws have been promulgated in recent decades and the need of modernization has gained notable momentum, it should be analyzed whether this new and widely international legal framework for security rights in movable assets has foreseen, actually embraced, or at least has not impeded the adoption of emerging technologies. The secured transactions legal system is composed of different parts. Therefore, the efficacy of the secured transactions system can be enhanced, not only by reforming legal rules, but also by a better coordination among its components, or the optimization of its operation as a whole. A sound, predictable, and workable legal system for secured transactions requires the conjunction of four elements. Those elements include legal rules, developed transactional and contractual practices, transparent and well-coordinated institutions—registries, courts, arbitration courts and other authorities, notaries—and a well-functioning market. Despite the modernization of the legal framework for security rights in movable property, if the other components of the system remain antiquated, poorly operational, or inefficient, the outcomes are unsatisfactory and the benefits of a modern legal regime frequently sink under the imperfections of the system as a whole. Digital-technology solutions can be applied to enhance the effectiveness of the system by perfecting transactional practice, refining institutional defects, reshaping registry models, streamlining enforcement procedures, or creating a well-functioning secondary market.[4] The expected benefits of law reform are only fully materialized after

3. See *infra* Part II for further elaboration on these assumptions, which are the starting hypotheses of this article.

4. As further explained *infra* Part III and Part IV. In relation to the proposition that digital technology can be a powerful enabler of a well-functioning secondary market by creating electronic-platform-based markets, previous works on electronic platforms illustrate this potential use as a market creator. Teresa Rodríguez de las Heras Ballell, *The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU*, 3 ITALIAN L. J. 149 (2017).

such a process.

This article has two objectives. First, the article examines how the incorporation of specific digital technologies to the different stages of secured transactions could mitigate the imperfections of the secured transactions system and enhance its effectiveness. To begin with, an envisioned integrated ecosystem of smart property and self-executed smart contracts for security agreements could effectively reduce verification and monitoring costs.[5] Next, a fully automatic electronic—maybe, blockchain-based—registry fed by a (IoT) network of interconnected assets would dramatically improve the accuracy of consistently-updated registered information.[6] Furthermore, implanted AI-based solutions could be used to detect changes of circumstances and deviations from agreed provisions.[7] Finally, AI-guided smart contracts could assist in decision-making to prevent breaches and automatically enforce remedies.[8] Second, given this backdrop, the article focuses on some of the legal implications for secured transactions legal system and assesses whether the current legal framework is prepared to face the challenges inherent to these new technologies, to exploit the multitude of opportunities presented by the technologies, and to manage the involved risks. Alternatively, if the current system is incapable of taking on this challenge, this article will consider an appropriate legal response.

With these aims, this article is structured as follows. Part II elaborates on the assumption that security rights are key market-failure-repairing mechanisms in modern credit-based economies and reveals the imperfections of the secured transactions legal system. Imperfections are particularly evident in four areas: visibility of security rights and priorities, monitoring, efficacy of enforcement, and realization of security right and value recovery. Further analysis in subsequent parts, however, will focus on technologies likely to enhance visibility, enable monitoring in dynamic transactions, and will only briefly address improved enforcement. Other areas are left to further studies. Part III outlines possible registry models for security rights and verifies their capacity to fit into existing international legal framework for secured transactions. In the analysis of the different registry models resulting from the incorporation of technological

5. Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 309, 324 (2017). *See also* Mark Giancaspro, *Is a "Smart Contract" Really a Smart Idea? Insights from a Legal Perspective*, COMPUTER L. & SECURITY REV. 1, 3 (2017); Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain* (MIT Sloan School Working Paper No. 5191-216, 2016), https://ssrn.com/abstract=2874598 [https://perma.cc/V4WH-S9UK].

6. Incorporating updated data fed by Oracles and Smart devices, Massimo Bartoletti & Livio Pompianu, An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns 1, 10 (March 18, 2017) (unpublished manuscript), https://arxiv.org/pdf/1703.06322v1.pdf [https://perma.cc/2B7R-93SX].

7. Harry Sunder, *Computable Contracts,* 46 U.C. DAVIS 629, 690–95 (2012) (automation enables detection of contradictions and allows non-human-intervention through computer-to-computer interaction). *See generally*, ERIK BRYNJOLFSSON & ANDREW MCAFEE, RACE AGAINST THE MACHINE: HOW THE DIGITAL REVOLUTION IS ACCELERATING INNOVATION, DRIVING PRODUCTIVITY, AND IRREVERSIBLY TRANSFORMING EMPLOYMENT AND THE ECONOMY (2012).

8. Raskin, *supra* note 5, at 331.

solutions, it will be revealed that whereas the implementation of electronic communications into notice filing, or registration, procedures is widely enabled and supported by the principles of functional equivalence and technology neutrality. Nevertheless, the escalation of automation in tasks fulfillment and decision-making, and the resort to decentralized models—in other words, blockchain-based—have a substantive impact on the legal effects attributed by the law to the legal design. Legal design can be implemented in practice through different architectures. Architecture describes a complex structure of functions, procedures, and relationships to which legal rules attribute specific legal effects. Therefore, whether a principle of architecture neutrality might be proclaimed is an important question that will be discussed. In sum, the article addresses whether architectures are neutral and, therefore, if any architecture can in principle satisfy the legal design. The answer is initially negative because a reshaping in architecture tends to result in a functional change departing from the legal design and its legal effects. Part IV tackles legal implications of smart contracts and their viability for articulating dynamic security agreements and self-enforcing post-default rights. Upon the verification of the legal feasibility of smart contracts, further analysis will be conducted within a hypothetical scenario of dynamic transactions, which are susceptible to periodic or permanent adjustment based on changes in relevant facts or the attendant circumstances. Subsequently, there is a brief discussion about whether self-enforcement, as the effectiveness-enhancing feature of smart contracts, is compatible with current legislation on the exercise of post-default remedies in secured transactions and the general legal principles. Part V summarizes the conclusions.

II
CREDIT MARKET FAILURES AND THE IMPERFECTIONS OF SECURED TRANSACTIONS LEGAL SYSTEM

Modern economies are highly dependent on the existence and the proper operation of a credit market. Nevertheless, credit markets are afflicted by market failures. The first of such failures is severe information asymmetries. The creditor has limited, and not always accurate, information about the debtor, the project, and the involved risks. Efforts to gather reliable information entail costs. The second failure is adverse selection. Difficulties with properly assessing the risk involved in competing projects penalize better projects and distort decision-making process towards non-optimal results. The third is moral hazard. The creditor cannot ensure that the credit will be used as intended by the receiver of funds or that the receiver will be duly vigilant in reducing risks, so post-closing monitoring measures are needed and risk exposure of the financial transaction increases.

Security rights constitute[9] legal solutions harnessed to correct market imperfections.[10] First, the creditor replaces the need of reliable information about the debtor's solvency and the viability of the project with the direct valuation of the collateral. Second, the realization of the collateral offers the creditor a route for credit recovery alternative to the project success. Accordingly, credit conditions improve and the impact of adverse selection diminishes. Third, because the exposure to inadequate use of funds or excessive risk taking is prevented by the value of the collateral, credit availability and access to finance in reasonable conditions heavily rely on a sound, reliable, and efficient secured transactions legal system. Secured credit strengthens creditors' position, minimizes risks involved in financing transactions, and fosters credit offers in efficient conditions

In sum, it is a widely-accepted premise, inspiring international harmonization instruments and triggering domestic reform of rules on security rights,[11] that a sound, effective, transparent, and modern secured transactions law would facilitate access to credit, mitigate risk exposure, improve financing conditions,[12] and reduce transactions costs.[13]

Significant and successful efforts have been and are still being made by international and regional organizations to procure harmonized rules on asset finance operations. As a result, a growing uniform legal framework on secured transactions is taking shape at the international scene. These efforts aim to promote cross-border activity, alleviate disparities[14] between legal traditions, provide credibility, and inspire domestic reforms to modernize antiquated rules, concepts and legal institutions. Examples of these harmonizing instruments include International Institute for the Unification of Private Law (UNIDROIT) texts (Cape Town Convention[15] and Protocols, primarily); UNCITRAL instruments (Legislative Guides and Model Law[16]), and texts from the European

9. *See* Steven L. Harris & Charles W. Mooney, Jr., *A Property-Based Theory of Security Interests: Taking Debtors' Choices Seriously*, 80 VA. L. REV. 2021, 2026 (1994) (some critical stances challenge the secured transactions system on a distributive basis, question the accuracy of market signaling, or warn of the risk of discrimination against unsecured creditors, an analysis of such concerns and reticent positions is found here).

10. Heywood W. Fleisig, *The Economics of Collateral and of Collateral Reform*, *in* SECURED TRANSACTIONS REFORM AND ACCESS TO CREDIT 81 (Frederique Dahan & John Simpson eds., 2008).

11. UNCITRAL, UNCITRAL LEGISLATIVE GUIDE ON SECURED TRANSACTIONS, at 1, U.N. Sales No. E.09.V.12 (2007) [hereinafter UNCITRAL LGST].

12. Boris Kozolchyk, *Secured Lending and Its Poverty Reduction Effect*, 42 TEX. INT'L L. J. 727, 728 (2007).

13. Anthony Saunders et al., *The Economic Implications of International Secured Transactions Law Reform: A Case Study*, 20 U. PA. J. INT'L ECON. L. 309, 344 (1999).

14. *See* Michael G. Bridge et al., *Formalism, Functionalism, and Understanding the Law of Secured Transactions*, 44 MCGILL L. J. 567, 664 (1998–1999) (divergences are not only patent in the lack of common rules, but more importantly in the existence of conflicting approaches to the whole system).

15. International Institute for the Unification of Private Law [UNIDROIT], Convention on International Interests in Mobile Equipment, Nov. 16, 2001, 2307 U.N.T.S. 285 [hereinafter Cape Town Convention].

16. *See e.g.*, UNCITRAL, UNCITRAL MODEL L. ON SECURED TRANSACTIONS, U.N. Sales No.

Bank for Reconstruction and Development (ERDB), the Organization for Harmonization of Corporate Law in Africa (OHADA), and Organization of American States (OAS).

Therefore, from a legal perspective, a secured transaction system is an effective stimulus for credit, as it mitigates risks and alleviates market malfunctions. Nevertheless, its efficacy is neither total nor absolute. The efficacy of the system in facilitating access to credit in competitive conditions depends upon the operation of the whole secured transactions system, a consistent fitting and coordination among all the components, and an effective functioning of every element. In effect, a sound, predictable, and operating legal system on secured transactions requires the conjunction of four elements: legal rules, developed transactional and contractual practices, transparent and well-coordinated institutions—registries, courts, arbitration courts and other authorities, public notaries—and a well-functioning market for secured credit. Consequently, in the absence of any such components, the existence of a legal framework does not suffice.

In practice, the legal system has failures as well. These imperfections debilitate the impact of legal strategies on the real market, undermine the capacity to repair market failures, and weaken the efficacy of legal solutions. In fact, transactions are fairly opaque for a number of reasons. Transparency is only partial and limited compliance monitoring is costly[17] and limitedly feasible. Active enforcement is complex and time-intensive, which reduces the deterrence effect. A full value recovery would depend upon the viability of remedies and, in particular, the existence of a well-functioning secondary market. Finally, rules are still fragmented, dispersed and, in some aspects, rather local.

Even if recent reforms and laudable harmonization initiatives have appreciably alleviated the imperfections arising from outdated rules, which have revealed themselves to be unsuitable for modern market practices, the enforcement of the system does inevitably present limitations. Some of them are inherently linked to current state-of-the-art procedures, institutions, and legal solutions.

A. Traditional Publicity-Providing Mechanisms in Secured Transactions and Their Limitations

The credit market is greatly stimulated by confidence. The perception of confidence in financial transactions depends upon the protection of reasonable expectations. Therefore, the credit market needs visibility. Opacity in secured credit system sends misleading or fully wrong signals to the market—in other words, false wealth.[18] As a consequence, confidence retreats from the market

E.17.V.1 (2016) [hereinafter UNCITRAL MODEL LAW].

17. Stephen D. Williamson, *Costly Monitoring, Loan Contracts, and Equilibrium Credit Rationing*, 102 Q. J. ECON. 135, 135 (1987).

18. SECURITY RIGHTS IN MOVABLE PROPERTY IN EUROPEAN PRIVATE LAW 8–9 (Eva-Maria Kieninger ed., 2004); Raghuram Rajan & Andrew Winton, *Covenants and Collateral as Incentives to*

scene or it is certainly misallocated. In this context, as security rights are intended to be—fully or to a limited extent—effective against third parties—provided that perfection/effectiveness requirements are met—signals have to be duly sent to the market. Therefore, secured transactions systems need publicity-providing mechanisms.

Traditionally, transfer of possession[19]—dispossessing the debtor—of the encumbered asset and registry systems[20] have been and still are in most jurisdictions the prevalent, although not the exclusive, publicity-providing techniques. Possession is an effective method for providing publicity in small societies and local markets with proximity transactions. But in a globalized market, the visibility scope of possession itself is undeniably modest.

Likewise, registry systems may be incomplete in scope and limited in visibility potential. They majorly, if not exclusively, operate on a consultation basis and under a centralized scheme; therefore, their efficacy depends on the availability, accessibility, and credibility of the registered information.[21]

B. The Cost of Monitoring

Monitoring is a costly and complex task in secured transactions. The administration of secured credit may require performance monitoring, assessing the fulfillment of agreed conditions, and audits of the existence and condition of collateral or control fluctuations in its value. Direct, regular, and *in situ* monitoring is in many transactions unfeasible, highly improbable, or extremely costly. Should monitoring ability be limited or unreasonably expensive, expected risks are higher and credit costs increased accordingly.[22]

As continuous monitoring of contractual performance is not feasible, transaction conditions are, in practice, unaligned with real risks and actual performance. In fact, a dynamic and permanent adjustment of terms is, in most market transactions, rather unrealistic. Whereas transactions naturally evolve and deploy their effects in medium or long term, contracts remain solidified in the original drafting. A continuous monitoring of the transaction and a resultant adaptation of the agreed conditions used to be materially unfeasible, economically unaffordable, and technically improbable.

Monitor, 50 J. FIN. 1113 (1995).

19. Giuliano G. Castellano, *Reforming Non-Possessory Secured Transactions Laws: A New Strategy?*, 78 MOD. L. REV. 611, 613 (2015).

20. UNCITRAL LEGISLATIVE GUIDE ON SECURED TRANSACTIONS 1, *supra* note 11, paras. 19–28, at 107–10

21. Helmut Bester, *The Role of Collateral in Credit Markets with Imperfect Information*, 31 EUR. ECON. REV. 887 (1987).

22. Efraim Benmelech & Nettai K. Bergman, *Collateral Pricing*, 91 J. FIN. ECON. 339, 341 (2009) (As empirical studies demonstrate in a market with information asymmetries, lenders need to conduct investigations into the debtors' financial position and control their activities until the debt is discharged to mitigate their exposure to risk. These investigations are costly activities. Accordingly, the cost of credit increases.).

C. Limitations in Enforcement

The ultimate rationale behind secured transactions is that the value of the encumbered assets is able to substitute for the recovery of funds in case of default or insolvency—by obtaining possession of the asset, disposing of it, or acquiring it, along with other possible remedies.[23] Accordingly, the enforcement stage is critical to ensure the effectiveness of the system. Should the creditors be unable to enforce their rights, repayment expectations are frustrated. Even more, when the enforcement is costly, complex, or uncertain, incentives to comply with the transactions are low and deterrence effect is weak. If the risk of default increases, credit conditions get worse.

Ensuring effective, quick, and simple enforcement is the biggest challenge in any secured transaction system. In practice, although the legal framework anticipates these situations and provide for solutions—sale or other disposition, collection, acquisition, public auction, realization agreements—the efficacy of the enforcement depends upon streamlined, fast and predictable procedures, effective remedies, and the existence of a competitive secondary market for the encumbered asset. Otherwise, the satisfaction of the creditor is insufficient and, sometimes, to a certain extent impracticable.

III
INNOVATIVE FEATURES FOR REGISTRY MODELS: AUTOMATIC, ELECTRONIC, AND DECENTRALIZED

A. Technological Architecture and Legal Design of Registry Models

Ensuring effectiveness against third parties (or perfection) of security rights is a critical value-creating and expectations-preserving element for secured creditors. Among available methods for achieving third-party effectiveness, most secured transactions legal systems, both at an international level[24] and at a domestic one, pivot on the registry model as the prevailing publicity-providing system for secured transactions, frequently along with the traditional possession-based method. Technological advances do, however, allow for an enhanced system. Technology developments could ameliorate the accuracy of the data provided by registries. In addition, digital technology could improve the trustworthiness of registries.

---

23. UNIDROIT Cape Town Convention, in force in seventy-three Contracting States, is an illustrative example with a wide catalogue of legal remedies to enable the recovery of funds in case of default. Cape Town Convention, *supra* note 15, arts. 8, 9 & 10.

24. UNCITRAL MODEL LAW, *supra* note 16, ch. III, art. 18. UNCITRAL Model Law provides for as primary methods for achieving third-party effectiveness (Article 18) the registration of a notice in the Registry and the possession of the encumbered asset by the secured creditor. Under the UNIDROIT Cape Town Convention, however, due to the specific characteristics of the categories of covered objects (unique identifiable, high-value, and mobile), third-party effectiveness is exclusively based on notice registration in an International Registry. Cape Town Convention, *supra* note 15, art. 5.

Regarding the expectations on data accuracy, an entirely electronic registry system, fed by data collected by IoT solutions—associated to objects, places, assets (smart property—could ideally provide dynamic, fully and automatically updated, perfectly—or highly—accurate, and all-embracing information related to secured transactions). First, data could be more updated if technology enables an automatic revision and update. Any subsequent change to registered data could be incorporated into the registration on an automatic basis. Information on location, technical specifications of the asset, level of use of the collateral, unexpected malfunctioning, deterioration, or loss would be detected, collected, and processed by the registry, and, where necessary, incorporated into the relevant record. Second, data could be more accurate, insofar as technology allows for the verification of the correspondence between the registered data and the factual situations at each time, to detect conflicting data, and to correct contradictions. An unauthorized change of location of the asset, a wrong description of the asset, or a filing conflicting with data provided by IoT devices could trigger a revision of the registration (notice) or even an automatic modification thereof.

As regards the level of reliability, the possibility of applying digital technology developments aimed to enhance the reliability of registered information and registries leads to a discussion of the role of registries as intermediaries and how technology impacts the efficacy with which such a role is performed. The key function of registries in the secured transactions system as publicity providers is indeed strongly associated to the role of intermediaries.[25] As a matter of fact, registries are authorized intermediaries that infuse credibility and confidence in market relations. As a consequence, a given legal system does usually link specific legal effects to registrations and the information thereby provided—authenticity, accuracy, right creation. Parties can trust each other because the information is trustworthy—it is reasonable to rely on the information or such a reasonable reliance is legally protected.

That intermediary-centered description corresponds to the registry model operating in some jurisdictions, whereas in others, a notice-filing model prevails. The notice filing model is most prevalent in common law countries but it is not exclusive to these countries; Latin-American countries have modernized their systems under the OAS Model Law.[26] A notice-filing registry model is faster, cost-effective, and more confidentiality-friendly; but it may be argued that this kind of registry projects a weaker trust in the market, as information has to be broadened, completed, or even confirmed in an out-of-registry context. Hence, trust is not assured by the legal design of the registry system and, then, risks have

25. *See* Teresa Rodríguez de las Heras Ballell, *Legal Aspects of Recommender Systems in the Web 2.0: Trust, Liability and Social Networking*, *in* RECOMMENDER SYSTEMS FOR THE SOCIAL WEB 43 (Pazos Arias et al. eds., 2012) (according to the theory of "layers of electronic intermediation," intermediaries provide accessibility, visibility, and credibility services).

26. Marek Dubovec, *UCC Article 9 Registration System for Latin America*, 28 ARIZ. J. INT'L & COMP. L. 117, 117 (2011).

to be covered or mitigated by other mechanisms, such as title insurance. That debate on the registry model is latent in the comparative law scene and has surfaced, with different intensity, in the context of harmonization projects on secured transactions.[27] From a technological point of view, in a pure notice-filing model, the main function of the registry is to provide, manage, and operate an electronic environment to collect, process, and give access to registered data. Human intervention in the process is mostly unnecessary or limited to certain inputs, tasks, or circumstantial contexts.

The open debate between the above-mentioned registry models intensifies with the incorporation of digital technology. As a matter of fact, although some countries have tried to preserve a registrar-managed model, the progressive shift towards entirely electronic registries seems to benefit notice-filing models. The extraordinarily successful International Registry for international interests in mobile equipment created under the Cape Town system responds to a notice-filing registry model that runs as a fully electronic registry with no registrar intervention. The policy option in the UNCITRAL Model Law[28] is conclusively preferring and encouraging electronic registries in access, storing, processing, and operation, within the context of a notice-filing model.

Therefore, the first question is whether an effective electronic registry needs necessarily to follow the notice-filing model and renounce the role of the registrar as a trust-creating intermediary. In sum, does the technological architecture impose a legal design and operation of the registry model? Even if it is obvious that the scope of automation is clearly wider and easier in a registry system where the control of a central registrar is more limited and the human intervention is less, the technological architecture does not necessarily determine a pre-defined model in terms of organization, principles, and procedures. Nevertheless, the resultant benefits in celerity and visibility and the expected efficiencies in costs might appreciably differ between registrar-managed registries and notice-filing systems.

Registrar-managed title registries can and should automatize areas and stages of the process, and implement electronic communication throughout the whole system without policy restrictions. It might even be argued that a title registry could be fully, or at least amply, electronic although at certain phases inputs are introduced or validated by human intervention, steps are double-checked, or final outcomes are somehow certified, reviewed, or controlled by the registrar. However, in imagining a model of interconnected smart devices that automatically collect and feed data into the registry, the feasibility of validation and its impact on efficacy can be questioned. If all data collected by smart

27. UNCITRAL LGST, *supra* note 11, paras. 29–33, at 110–11. Jorge Feliu Rey, *El Derecho de Garantías Mobiliarias en Contexto: Una Aproximación Global*, 29 LA LEY MERCANTIL, 1, 6 (2016) (explaining how the diverging evolution of legal traditions—formalist and functionalist—on secured transactions has also been associated with a different role of registry and, accordingly, to differing registry models—title registry versus notice filing).

28. UNCITRAL MODEL LAW, *supra* note 16, ch. IV, art. 28.

property have to be subject to prior scrutiny and validation by the registrar, the system could be overwhelmed by a permanent flow of data. Accordingly, the incorporation of the data into the notice would delay, registered data would not be fully updated, and, then, reliability of records would dramatically plunge. As a consequence, the benefits in rapidity, immediacy, and full publicity associated with automatic collection of data dilute.

A total automation of validation processes, authorization tasks and interaction leads to a more complex scenario. Beyond the implementation of electronic communications and the automation of certain stages of the registration process, the question is whether a totally automatic registry is compatible, operating without human intervention, with the substantive effects assigned by the law to tasks traditionally entrusted to (human) registrars—qualification and certification, denial or granting of access, interpretation. It has then to be argued whether the requirement of human intervention is inevitably presuming the acceptance of a level of discretion that would impede any automation attempt and, accordingly, whether such a discretion should necessarily entail a degree of subjectivity incompatible with non-human actions. Or whether the real unique value of human intervention does indeed stem from the fact that human decisions are not outcomes of purely rational-based course, but an amalgam of varied rational and non-rational factors, something very difficult to replicate in non-human processes.[29] If, however, the human intervention is not understood, nor even conceived, as a discretionary or subjective decision, but rather it is assumed that the human decision-making is framed by a set of rules, that it reasonably applies standards, duly assesses relevant facts, and issues a balanced and well-founded decision, the possibility of codifying these tasks and steps in a AI-guided automatic process appears feasible, likely, and really attractive. Should criteria and standards to decide be pre-determined in sophisticated AI devices, the compatibility of automatic registries with the legal design of registrar-conducted models seems higher and more probable.

Notice-filing systems would seem to be better prepared to exploit the efficiencies of the ecosystem of smart devices connected to the registry. As validation is not required, data fed by smart devices would immediately incorporate in the notice, update the information, and be readily accessible. Despite those evident benefits, the risk of a massive flow of data feeding the system might endanger effective performance. Notice-filing systems serve to warn market participants who should investigate further to corroborate the information and get relevant details. Should a permanent flow of data clutter the record, its main function could be obscured. Over-information-providing registries could seriously misinform interested parties. The red-flag function is essentially based on concision, relevance, and manageability. Automatic

29. Harry Surden, *Values Embedded in Legal Artificial Intelligence* (U. of Colorado Law Legal Studies Research Paper No. 17-17, 2017), https://ssrn.com/abstract=2932333 [https://perma.cc/XAT7-NETD].

collection of data should be then carefully selected and maybe screened.

Furthermore, under both title registries and notice-filing systems, other legal concerns and practical considerations exist. The efficacy of the system depends upon a well-functioning technological infrastructure that interconnects systems, devices, and platforms controlled by different individuals and entities. If there is any failure or malfunctioning, liability issues will arise. Who is responsible for keeping smart devices in proper operation and duly connected to the registry? Who should implement security measures? How should security vulnerabilities in smart property be detected? Should error-detecting or report mechanisms be implemented? Likewise, if the collection of data and its subsequent incorporation into the record are automatic, consent-related issues emerge. Data might be collected and incorporated into records without authorization of relevant parties. It must be explored whether an advance general consent given by the registrant, or the debtor, to the further automatic addition of data, without prior control or approval, would suffice. Maybe, the relevant parties in each record should approve the connected active smart devices in advance. Or, a quick authorization mechanism for each entry could be deployed. All these technical considerations and practical matters prove the need for profound rethinking of legal design in the light of emerging technological architectures.

B. From Functional Equivalence to Architecture Neutrality?

The discussion above leads us to assess the extent to which existing legislation on secured transactions, electronic commerce, and register-related issues embraces a fully-electronic highly-automatized registry system for security interests. To date, such a compatibility assessment has been conducted under the enabling principle of technological neutrality and functional equivalence.[30] The implementation of technologies into the relevant legal situations—registration, cancellation, modification, search, manifestation of consent, submission, notice filing—did not alter the legal design of the registry in each jurisdiction. Technology is simply an enabler of legal solutions. Today, the effect of implanting of technology is more disruptive. Technological solutions can reshape the legal design. Then, the conundrum gains more complexity. Should legislation have attributed certain legal effects to the operation of the registry in conformity with the legal design, a reshaping of that legal architecture by effect of technology may have substantive effects. Architecture would not be neutral. So, if the law provides for registrations that are deemed valid and accurate because the registry operates under a registrar-supervised model and the registrar is entrusted with the revision and qualification of the information to be registered, the transformation of the registry into an electronic automatic model without human intervention affects the legal design and the legally recognized effects might lose

30. These principles are enshrined in UNCITRAL MLEC, UNCITRAL MLES, UNCITRAL CEC. *See supra* note 1 and accompanying text. These principles have guided the subsequent instruments adopted by UNCITRAL. *See, e.g.*, UNCITRAL, UNCITRAL MODEL LAW ON ELECTRONIC TRANSFERABLE RECORDS, U.N. Sales No. E.17.V.5 (2017).

justification.

For the purposes of that analysis, it is necessary to infer from legal provisions the prevailing legal designs of the registry models and their operation to ascertain whether current legal design is prepared to embrace these innovations and to what extent existing rules may still work in electronic automatic registers.

1. Electronic and Automatic Registers

In broad strokes, without diving into legislative details and institutional peculiarities in each jurisdiction,[31] a secured transactions registry is traditionally depicted as a bidirectional scheme that collects information provided by eligible users (registrants) and makes selected information accessible, to the public or by request, by the registry. Therefore, registration, amendment, cancellation, or any other prescribed actions are triggered by a notice submitted by the registrant to the registry[32] or, if regulated so, undertaken *ex officio* by the registrar.[33] As a consequence, risks and liability related to the accuracy of data, the completion of the registration, the time of effectiveness, the compulsory cancellation, or the need to amend are clearly allocated on each position of the communication system, either on the registrant—secured creditor, person identified, or another person entitled thereby—or on the registry.

The above-envisioned possibilities of automation reshape the operational logic underlying traditional registry models subject to the current state-of-the-art limits. At least three situations seem to potentially conflict with the notice-based scheme of data flow. First, if, with the support of IoT solutions and smart devices, the registry may verify the accuracy of the registered data[34] or fill the gaps of an incomplete registration, liability allocation, duties of the parties, and notice rejection rules may be affected. Second, should a registration be automatically amended, or cancelled[35] on the basis of the information collected by smart devices and fueled into the registry system, rules governing who is entitled to submit such notices, when to submit them, and the consequences of failing to submit turn out to be irrelevant. More importantly, an automatized registry becomes more accurate, reliable, and autonomous, but parties' decisions are excluded from the system, unless it would be assumed that a general consent is given in advance. Third, a Registry based on a search-request model[36] displays in practice a limited visibility capacity. It is essentially passive. Information is stored in the registry

31. To that end, the subsequent analysis in the text is based on the Model Registry Provisions (MRP) included in the UNCITRAL Model Law instead of in specific domestic rules. So, some references to certain articles of the MRP will be scattered along the discussion to act as model provisions defining a global stereotyped model for a secured transactions registry. *See* UNCITRAL MODEL LAW, *supra* note 16, at 17.

32. As an exemplification, see *id.* at 19, 26 (arts. 5 & 16).

33. *See id.* at 20, 23 (arts. 6, 7, or 13.2).

34. *See id.* at 31 (art. 24).

35. *See id.* at 27 (art. 20) (automating, for instance, the compulsory registration of amendment or cancellation notice situations laid down here).

36. *Id.* at 20 (arts. 22 & 23).

databases and available at request of the searcher. An electronic registry, however, could automatize the sending of messages to interested parties, the adoption of proactive actions, and the activation of warnings to ensure awareness.[37]

Then, real publicity increases and awareness presumption becomes more credible, insofar as the function of the registry would not consist simply in ensuring accessibility, but actually in informing of relevant information to interested parties. Such a proactive informative registry would require to operate an interwoven infrastructure of interconnected institutions, authorities, contracting parties, smart contracts and property, and raise a succession of legal concerns related to privacy, confidentiality, or party autonomy. Hence, all these possible scenarios have to be imagined to test whether existing legal framework is prepared to embrace these promising registry models, or, contrariwise, a profound reshaping of our legal archetypal models for registries is imperative.

2. Decentralized Registry Model

In addition to the debate above, nascent blockchain technology adds another disruptive element, another radical change in the architecture: from a centralized registry model that relies on the concept of trust-generating intermediary, to a decentralized registry model with a high level of (distributed) confidence but without the participation of a central entity. Promising prospects have been linked to the implementation of distributed-ledger schemes in different sectors and for a variety of purposes, other than its popular use in the Bitcoin architecture.[38] It is very pertinent to dive into the prospective uses of that technology for registration and publicity purposes. Far beyond the most obvious implications in terms of structure, a number of issues derive from a possible reshaping of registries under a decentralized scheme: privacy, control and management, authority and power, data accuracy, legitimacy, geographical scope, to name a few.

Unlike current centralized registry system, blockchain technology applications force us to think about the advantages of a registry system supported by distributed ledger technology when exploring an optimal design of a fully electronic registry system of global scope for secured transactions.

37. *See id.* at 26 (art. 15) (reflecting a very limited approach to the proactive role of the Registry).

38. EUROPEAN PARLIAMENT, HOW BLOCKCHAIN TECHNOLOGY COULD CHANGE OUR LIVES (2017), *available at* http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf [https://perma.cc/EX2X-UJSU]; Joseph Bonneau, et al., *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, IEEE SYMP. ON SECURITY & PRIVACY, 104, 118 (2015), *available at* https://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf [https://perma.cc/2VBR-ELJE] (analyzing the multiple functionalities of Bitcoin).

In light of the principle of technology neutrality,[39] legal effects will not be denied to data messages stored in blockchain schemes. Likewise, where specific requirements are laid down in the legal texts, like writing, signature, original, and offer or acceptance, for the purposes of recognizing functional equivalence, blockchain technology will not impair the ability of data messages to meet legal requirements. Therefore, blockchain is neither excluded nor contrary to existing legal rules on electronic commerce. Such reasoning endorses the above-proposed transition from paper-based registries to electronic ones. Functional equivalences for registrations, the act of registering (filing a notice), accessing, modifying or cancelling, the searchability of the registration, or the receipt, the sending, and the search are easily translated in a blockchain-based scenario. Interestingly, in relation to certain requirements like integrity, blockchain is particularly suitable for ensuring reliability and immutability. Up to this stage, the absorption of blockchain challenges into the existing electronic commerce legal framework has been smooth. The main reason of such a placid incorporation into the legal system is due to fact that current rules on electronic commerce are essentially transaction-oriented.[40]

Nonetheless, blockchain also impacts structures. In fact, distributed ledgers on a public blockchain depicts a decentralized model without a trust-generating central body. "The block chain is not maintained by any single entity, but instead relies on a mathematically innovative consensus mode."[41] Innovation in architecture constitutes a greater challenge to accommodate blockchain technology into existing rules. Model Registry provisions (MRP) within UNCITRAL Model Law on Secured Transactions (Model Law) are imbued by the prevalent model of a centrally administered registry.[42] Despite the aspiration for technology neutrality, it can be affirmed that, in general terms, Model Law provisions seem devised for centralized registries and, therefore, might be ill suited for decentralized models.[43] The need for specific rules should be explored.

---

39. UNCITRAL MLEC, *supra* note 1, *Guide to Enactment*, par. 46, at 31 (explaining, in the commentary to Article 5 on Writing, the principle of technology neutrality, frequently interpreted as a principle of non-discrimination. As per the principle of technology neutrality or non-discrimination, laws should not treat paper documents and data messages differently. More generally, legal rules should not discriminate on the grounds of the technology used and should remain neutral in the treatment and the attribution of legal effects irrespective of any technology used).

40. Teresa Rodríguez de las Heras Ballell, *Rules for Electronic Platform: the Role of Platforms and Intermediaries in Digital Economy, A Case for Harmonization*, UNCITRAL FOURTH INT'L COLLOQUIUM ON SECURED TRANSACTIONS (2017), http://www.uncitral.org/pdf/english/congress/Papers_for_Programme/139-RODRIGUEZ-Rules_for_Electronic_Platforms.pdf [https://perma.cc/3WEA-A4WU] (last visited Sept. 28, 2017). *See also* Teresa Rodríguez de las Heras Ballell, *The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU*, 3 ITALIAN L. J. 149, 153 (2017).

41. Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805, 814 (2015).

42. *See* UNCITRAL MODEL LAW, *supra* note 16, at 35 (art. 17).

43. *See* Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (March 10, 2015) (unpublished manuscript), https://ssrn.com/abstract=2580664 [https://perma.cc/6XJP-T4A2] (as blockchain-based smart contracts do not depend on a third party to

IV

DYNAMIC AND SELF-EXECUTED SECURED TRANSACTIONS IN AN ECOSYSTEM OF SMART PROPERTY AND SMART CONTRACTS

Digital technology—IoT,[44] especially, and smart contracts—offers solutions that would enable the creditor to use a cost-effective and permanent monitoring of the performance, a close tracking of the encumbered asset, and even a supervision of debtor's behaviors. That would allow the creditor to personally and directly supervise the compliance and immediately detect a default or an infringement—unauthorized sale of the collateral, change of location, deterioration of the asset, downgrade of rating, material adverse changes, other event of default—and, more interestingly, it would disincentive, make costly, or even make it technically unfeasible to breach,[45] or, if it occurs, self-execute remedies.

Hence, should technology enable parties—primarily, creditors, but also authorities, co-debtors or third parties—to collect and receive permanent updates of the performance status—location of the asset, physical condition, uses of the collateral—to process data fed by IoT solutions associated to the asset (smart devices) with other relevant information affecting the transaction—other loans, changes in rating, news on debtor's activities, etc.—fed by so-called "oracles,"[46] and to assess on an automatized basis the impact of such circumstances on the contractual terms, dynamic transactions could be a reality. Interest rates, penalty clauses, risk assessments or expected breach could be assessed on a dynamic basis and evolve within predetermined ranges in conformity with an AI-based decision-making process.

Three areas of interoperation between IoT solutions and smart contracts, integrating a more and more complex ecosystem of smart devices, (blockchain-

operate and cannot be controlled by anyone).

44. *See* INT'L TELECOMM. UNION, SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS (2012), *available at* http://www.itu.int/rec/T-REC-Y.2060-201206-I [https://perma.cc/P48B-EDCL] (The Internet of Things (IoT) has been defined as "a global infrastructure for the information society, enabling advanced services by interconnecting [physical and virtual] things based on existing and evolving interoperable information and communication technologies"); INT'L TELECOMM. UNION, ITU-T SG20: IOT AND ITS APPLICATIONS INCLUDING SMART CITIES AND COMMUNITIES (SC&C), http://www.itu.int/en/ITU-T/studygroups/2013-2016/20 [https://perma.cc/BEF9-55CH] (last visited Nov. 17, 2017) (The Global Standards Initiative on Internet of Things (IoT-GSI) concluded its activities in July 2015 following TSAG decision to establish the new Study Group 20).

45. Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY (1997), http://firstmonday.org/article/view/548/469 [https://perma.cc/AD8Z-T6CQ] ("The basic idea behind smart contracts is that many kinds of contractual clause . . . can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher.").

46. *See* Stefan Thomas & Evan Schwartz, *Smart Oracles: A Simple, Powerful Approach to Smart Contracts*, GITHUB (July 17, 2014) https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts [https://perma.cc/5KX3-456P] ("Smart oracles build on the idea of oracles, or entities that provide smart contracts with information about the state of the outside world, and combine information gathering with contract code execution.").

based) smart contracts and humans can be discussed. First, connected devices could capture and direct precise and updated data into smart contracts in the formation stage in order to specify assets, locations, or parties' details. Second, smart or connected devices could help to detect subsequent changes in a set of pre-defined data and allow smart contracts to adapt agreed conditions in accordance to the new circumstances. Third, smart devices could interact with the smart contract in case of breach of contract on a bidirectional basis: collecting data that upon incorporation into the contract prove non-fulfillment as well as reading the state of blockchain and reacting as agreed with a programmed response of the smart property, in other words, ignition suspension in case of delayed payments. Basically, the network of smart devices and oracles would ensure a permanent flow of data throughout the lifecycle of the contract, whereas smart contracts would enhance efficiency, speed, and performance of transactions.

A. The Legal Viability of Smart Security Agreements

Before elaborating on the discussion, tackling an essential preliminary question is imperative. Under the relevant international legal instruments, security rights are created by a security agreement. Are the fundamental principles on electronic commerce sufficient to declare that a smart contract creating or providing for a security interest is a functional equivalent of a security agreement, provided that the remaining legal requirements are met—namely, power to dispose, identification, sufficient description, determinability of secured obligations, or even in writing, where stated by law? Whereas these principles have sufficed for the earliest versions of electronic contracts at their primal stage, it is arguable whether smart contracts are simply a maturation of electronic contracting with the devising of more sophisticated artifacts, or if they usher in a totally novel era for contract law that maybe presages its disappearance by replacement. Like many other technological phenomena, there is not a universally accepted definition of smart contracts, and the evolution of market solutions and technological products produces varied changing descriptions. For the purpose of this work and the subsequent analysis, smart contracts will be defined as a process of automation of different phases of agreements—pre-contractual, formation, performance, enforcement—by digital codification, in a computable obligation. Such a comprehensive and evolving definition allows it to extend the following discussion from basic self-executed and self-enforced smart contracts to more sophisticated smart contractual processes that may include the automation of negotiations or, eventually, of conflict dispute resolution alternatives as well.

Unlike the gamut of electronic contracting types, smart contracts seem not only to affect the form but also to hit the substance. Are smart contracts actually contracts?[47] Even if the vertiginous progress of technology and, in particular, the

47. Kevin D. Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 338 (2017).

fascinating possibilities of AI may very soon make the following response incorrect and unbearably simplistic, it is worthwhile having the discussion now and reopening the debate again when circumstances have changed. At the moment, this article assumes as valid that smart contracts codify an agreement between the parties that has to exist, although not necessarily it must be a previous and separate agreement.[48] Therefore, although the agreement is initially and solely written in machine-readable language, it represents, expresses, and implements a meeting of minds' or another legally enforceable promise. Otherwise, it should be admitted that smart contracts would be replacing legal agreements and challenging contract law basis.

Even departing from the above-proposed assumption, legal concerns proliferate. As the code is not an expression of a previous oral or written agreements, as it occurs in the most primitive versions of electronic contracts, it has to be debated whether it would fulfill the legal requirement of being in writing, and, concurrently, how the contracts will be interpreted. Likewise, standard-terms-like problems related to transparency, knowledge, and genuine consent for incorporation of non-negotiated terms seem to revive here, due to the singularity of the drafting (coding) process. At the same time, the assumption that smart contracts are in practice coded agreements immediately reveals the apparent limitations of smart contracts compared to traditional contracts. It is not unreasonable to suspect that provisions cannot be efficiently coded if terms are ambiguous, require an act of discretion, or are based on indeterminate legal concepts—reasonable manner, good faith, best efforts. Therefore, it could be concluded that smart contracts tend to enable the automation of only certain kinds of transactions or discrete elements of complex transactions, but they may be unable to fulfill the role of traditional contract in governing a complex transaction in its entirety. As a consequence, an attempt to make a smart contract operable could lead to a simplification of the agreement by annulling nuances or avoiding the controlling role of general principles, or, interestingly, to a reformulation of terms drafting. Thus, an obligation to keep the asset in good condition could be reformulated in a smart contract as the duty to meet the maintenance schedule and report any defect. Besides, an expected sophistication of AI-based solutions in smart contracts would progressively mitigate such a limitation and expand their potential uses and applications. The data processing and assessment capacities of AI-conducted devices anticipates in the very near future the availability of smart contracts able to evaluate complex social situation,

48. *See* Primavera De Filippi & Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, FIRST MONDAY (Dec. 5, 2016), http://firstmonday.org/ojs/index.php/fm/article/view/7113/5657#author [https://perma.cc/WVA8-FWSR] (The premise here is that the own coding process does simply convey an agreement or a legal obligation that support the enforceability of the code. The authors do, however, seem to nuance that assertion when they state "the most recent blockchains have introduced the ability for people to upload small snippets of code (so-called *smart contracts*) directly onto the blockchain, for them to be executed in a decentralized manner by every node of the network. These rules are automatically enforced by the underlying technology, even if they do not reflect any underlying legal or contractual provision").

apply indeterminate legal concepts, and adopt decisions with ambiguous inputs.

Against this backdrop, the following diagnosis may be issued. Provided that legal requirements such as power to dispose, identification, description are met, smart contracts can validly create or provide for security rights. The formal requirement of being in writing could be overcome accepting that the code is an expression of the agreement. However, such a view could be too simplistic. It should be inquired into the legal functions attributed to "in writing" requirement. Overall, the writing formal requirement seeks to serve for evidentiary purposes, to ensure a subsequent accessibility of the terms, to enable interpretation, or to protect a weak party upon the drafting and the incorporation of standard terms by the other party. Then, whether the code achieves the same functions as writing does, in any medium, must be decided. To the extent that it is retrievable or readable through an interface, the ability to fulfill the said functions should not be discarded. Accordingly, smart security agreements would fit into current international rules on secured transactions.

B. Dynamic Secured Transactions Based on Smart Contracts and Smart Property

Monitoring represents a significant transaction cost in business activity. In secured transactions, the performance of the debtor, the subsequent change of circumstances affecting the collateral, and the modification of other relevant factors are likely to increase the risk, but they need to be monitored and incorporated in the contractual process in an efficient manner. Concurrently, should monitoring be feasible and reasonably effective, adaptation of the contract provisions to new circumstances has to be possible, must be foreseen in the agreement, and needs well-established mechanisms to assure predictability. Traditional contracting practices are not suitable therefor.

Smart contracts, together with a network of relevant smart devices and oracles, however, allow for the design and regulation of dynamic transactions. Their legal feasibility is essentially rooted in the existence of sufficient agreement of the parties in the initial selection and definition of conditions to be adjusted, data to be collected, criteria under which terms will be adapted, and limits of the agreement modification. This would work as a multiple-scenario or modular agreement where parties anticipate several future scenarios and define different set of conditions for each situation. Instead of agreeing on static conditions, parties would define a range of possibilities for those conditions subject to periodical or permanent adaptation—interest rate, repayment period—data, circumstances or facts triggering the adaptation of terms—level of use, compliance of maintenance obligations, location of the asset, credit rating—and legal consequences—change of economic conditions, increase of interest rate, breach of contracts, enforceability of penalty clause/liquidated damages clause. If all these conditions, limits, ranges, and consequences are fixed and agreed upon in advance, the contracting parties would be validly defining a framework for the modification of the contract where the decision to amend the initial contract is

articulated by implementing a mechanism—smart property collecting and processing data—for modification. All the amendment outcomes would be determinable. Once the agreed criteria are met, modification of contractual terms is automatic and would not require a further specific agreement of the parties. From this perspective, no specific legal action would be required to deem dynamic contracts agreements valid and enforceable within the current legal system. Their feasibility will entirely depend upon adequate drafting and skillful contractual practices. Nonetheless, due to the complexity of the contract and the fluctuation of applicable terms and conditions, the possibility of configuring a right to be informed or a positive duty to inform other parties to the contract about the status of the contract might be seriously considered.

C. Self-Executed Remedies and Self-Help Measures in Secured Transactions

Self-enforced smart contracts can enable remote-control actions likely to affect goods, persons, or services. For example, consider the self-help effects of deactivating passwords to access services, suspension of access, removal or unavailability of content, blockage of funds, ignition suspension, down grading of rating, change of profile, and geolocation-related actions. All these technical actions constitute self-enforced remedies against default.

Secured transactions could be significantly enhanced by effectiveness in enforcement. This could enable an extremely satisfactory repossession by an automatic and immediate transfer of control over the collateral—password, digital keys, or other identification factors—an expeditious disposition of the intangible assets or rights—value transfer, settlement—or the conclusion of a lease or license agreement as a post-default remedy by the automatic coding of a new smart contract for those purposes.

The resort to automatic, self-executed remedies implemented through an ecosystem of smart contracts and smart devices is neither expressly contemplated in current legislation, nor even considered at the time of the drafting of legal rules. Nonetheless, it might be tested whether they are compatible with legal requirements, as functional equivalent solutions, or at least resist a scrutiny of general principles (abuse of right, good faith, reasonableness, antisocial exercise of right, violation of constitutional rights, public order).

Under secured transactions laws,[49] post-default remedies can be provided by the security agreement or specified by the law. Additionally, creditors are entitled to exercise their rights in case of default by judicial or extrajudicial methods. If rights are exercised without application to a court or other authority, certain requirements might have to be fulfilled to protect debtors' and third parties' interests—giving notice, specifying procedures, adequate method, good faith and commercial reasonableness.[50] These examples help to surface some

49. For an illustration of a standard rule see UNCITRAL MODEL LAW, *supra* note 16, at 61 (art. 72).

50. As required, for instance, by Article 78 UNCITRAL MODEL LAW for disposing of the encumbered asset, after default, without applying to the court. UNCITRAL MODEL LAW, *supra* note

concerns in relation to self-executed smart contracts to enforce security rights. Remedies should be provided for by the security agreement or specified in the applicable law and, if multiple sources inform remedies, they should be exercise in a compatible way. The self-execution of automatized remedies in smart contracts could neither disregard nor elude legal requirements for the exercise of the relevant post-default rights. Critical points are numerous: if due notice of the default and secured creditor's intent to dispose or repossess is given, if the person in possession has the opportunity to object to repossession in case of automatic enforcement, if a proposal for the acquisition of the encumbered asset is sent, if the grantor has consented to the collection of payment, among others.

The traditional functional equivalence principle could assist in the fulfillment of many requirements—notice can be generated automatically, the person in possession could be warned by any electronic communication and, if he/she objects may technically impede the execution by prohibiting the transfer of passwords to control, and then repossessing the encumbered object. However, automation has other more substantial repercussions in the protection of rights and the access to justice. First, automation requires accepting the generalization of self-help measures. Second, judicial and extrajudicial proceedings are not today suitable for settling disputes and attending claims with such celerity, as automation can. As a consequence, the possible harm on rights and interests caused by the application of self-help measures are not effectively compensated, and can endure unreasonably or even become irrecoverable due to a belated judicial/extrajudicial resolution. The automatism of the self-enforcing effect should be compensated by the availability of expeditious proceedings to complain, a better reporting system, or speedy injunction options, even those requested and issued through electronic means, for example, within electronic platforms.

From a regulatory point of view, three paths can be taken. First, there could be a radical prohibition of smart contracts and smart devices in the field of secured transactions. This shortsighted approach would likely hamper innovation and deprive transactions of numerous possibilities to enhance effectiveness. Second, a reconciling position could emerge stating that automatic performance and self-executed enforcement are in conformity with the law insofar as they comply with legal requirements and seek to protect parties' interests. Such a reasonable stance leads accordingly to the conclusion that smart contracts in combination with remedies-enforcing smart devices should be devised, developed, formulated, and coded to implement equivalent solutions to comply with legal requirements—notice giving, opportunity to object, value assessment. Certainly, that might negatively impact expected celerity and retard effectiveness of automatic and self-executed remedies, impede the automatization of certain areas or stages of the transactions, and limit the coding process to unambiguous, non-discretional, and unequivocal provisions. In practice, innovative strategies to

16, at 63 (art. 78).

refine the coding and enhance the design of smart contract/smart property environment will be encouraged. Third, a final position expressing discontent with the existing legal framework that would be deemed ill-suited for embracing the overwhelming innovations in the realm of smart contracts and smart devices. From that perspective, the adoption of new specific rules to clarify the validity and enforceability of such technological developments and set out standards and requirements to be met would be necessary and imperative to consolidate the innovation track

V
CONCLUDING REMARKS AND PROSPECTIVE ISSUES

The advent and quick expansion of technological developments such as smart contracts, IoT, AI solutions or blockchain are not simply continuing the natural expansion and progressive consolidation of our digital society. The fascinating possibilities that these technologies promise and the disruptive effects that they announce reveal that the impact will be more radical and transformative. This article argues that this second wave of technological progress ushers in a second generation of digital law. This new wave represents the need to develop a different legal approach to technology. To date and throughout the last decades, the legal response and, consequently, the legislative production has been successfully driven by the conciliatory principles of functional equivalence and technology neutrality. In the face of arriving technologies, these principles start to show some signs of exhaustion, which encourages exploration in the formulation of new principles or at least reconsideration of the scope of the current ones. To test that assertion, this article suggests a technological scenario likely to trigger such a debate about how to face technological challenges, which legal tools—both principles and rules—we have and what we need. It has envisioned an ecosystem of self-executed smart contracts, smart property, and humans, with a high degree of interconnection, an increasing level of automation, and an expanding resort to AI solutions progressively applied to all stages of decision-making.

Such a technological scenario tries to capture the idea that today's technologies are largely changing the context for business transactions and social relations. It is then a matter of scale. First-generation digital law provides for rules recognizing legal effects of electronic signatures, contracts concluding by electronic communications, or control-based mechanisms equivalent to possession. Current digital law solves single legal problems one by one. The challenge for the second-generation digital law is to ascertain whether the entirety of the legal system is prepared to embrace legal situations that take place within the complex ecosystem of the above-described hypothetical scenario. It is a question of architecture. Are architectures neutral from a legal perspective? Can same rules be applied in different ecosystems that define different social architectures? Whereas functional equivalence and technology neutrality smoothly work in the former situation, the latter scenario advises to reconsider

them.

The combinations of technologies, as described in the hypothetical scenario, show fruitful synergies and feedback effects. Secured transactions becomes faster, dynamic, and more predictable; publicity-providing methods for security rights improve their accuracy and completeness; performance is monitored and infringements prevented; effectiveness of enforcements dramatically enhances with streamlined procedures, automatic responses, and self-help measures. The prospects are almost utopian. A secured transactions legal system repairs its imperfections and takes the road to perfection. Would perfect technology replace imperfect law?

In conclusion, the existing rules on secured transactions apply to the depicted scenario to the extent that functional equivalence and technological neutrality works well. This means that new technologies could be integrated to strengthen the current legal framework sustaining secured transactions without requiring a substantial overhaul. This emerges from the analysis of filing systems, which could be automatized to the benefit of their users streamlining the procedures for accessing secured credit. Deeper reconsiderations, however, are necessary when the application of disruptive technologies is applied too generally, depicting an ecosystem of smart contracts, smart property and humans. In a world where all agreements are self-executed and self-enforced, concerns related to access to justice, protection of fundamental rights, irreparability of damages, or abuse of rights reappear. Hence, the legal framework sustaining secured transactions should match an entirely new architecture.

In light of these observations, a roadmap for policymakers could be identified. At an initial stage, legal rules could accommodate new technologies under the principles of technological neutrality and functional equivalence. Then, at a subsequent stage, when technology will inevitably reshape the building blocks of societal interactions, functional equivalence should be abandoned. Focusing only on the first stage is shortsighted. Architecture-oriented principles should be developed. Those entail, inter alia, a profound rethinking of the very concept of contract and its role in society, a recalibration of remedies, the setting of standards for AI-based decisions to be valid and enforceable, the refashioning of dispute resolution mechanisms, and the incorporation of technologies in prevention and civil enforcement.