US-China Law Review, March 2018, Vol.15, No. 3, 139-149
doi:10.17265/1548-6605/2018.03.003

The Normative Role of Smart Contracts

JIANG, Jiaying
Emory University School of Law, Georgia, USA

Smart contracts are agreements whose execution is automated by computer codes that translate legal prose into an executable program. They are designed to ensure the performance of agreements automatically, without human involvement. Smart contracts have received tremendous attention lately as it could bring about the enormous impact to many industries that will revolutionize business and redefine economics; smart contracts also have created the fear that they would overturn the legal industry and displace millions of legal jobs. Therefore, it is critical to first identify the role of smart contracts in the current legal system and explore mechanisms for smart contracts to better serve the legal research, legal practice, and legal professionals, not to displace the legal industry thoroughly. In this article, the author proposes that smart contracts assume an instrumental role aimed at serving the current contract law system, instead of trying to become an alternative to that system. Embedding smart contracts within the current contract law system, which they function as a tool, represents a situation with considerable more potential for success. The success would derive from smart contracts' value of increased efficiency. With such value, the author further proposes three guidelines for enhanced instrumental functionality within the existing contract law system from three perspectives, including specification of areas of application, technological improvement, and legal support.

Keywords: smart contracts, normative role, value of increased efficiency, guidelines for improvement

Introduction

Smart contracts are agreements whose execution is automated by computer codes that translate legal prose into an executable program (Raskin, 2017). They are designed to ensure the performance of agreements automatically without human involvement.

Smart contracts have received tremendous attention lately because they have been found capable not only of automating a contract's execution, but also of being utilized in various industries. For instance, smart contracts can automate compliance by digitalizing Uniform Commercial Code (UCC) filings and automating their renewal and release processes.[1] In the securities market, smart contracts can facilitate the automatic payment of dividends, stock splits, and liability management, while reducing counterparty and operational risks (Szabo, 1995). In trade finance, smart contracts can facilitate streamlined international transfers of goods through faster Letters of Credit and trade payment initiation, while enabling higher liquidity of financial assets (Szabo, 1995). Other than that, smart contracts have been proposed for various uses, such as derivatives, government records, auto insurance, and supply chain management.

Jiang, Jiaying, Candidate of Doctor of Juridical Science, Emory University School of Law, Georgia, USA.

[1] Smart Contracts—12 Use Cases for Business and Beyond—Chamber of Digital Commerce, http://www.the-blockchain.com/docs/Smart%20Contracts%20-%2012%20Use%20Cases%20for%20Business%20and%20Beyond%20-%20Chamber%20of%20Digital%20Commerce.pdf (last visited January 2, 2018).

While these proposals seem to be premature, the legal profession nonetheless remains mostly unaware of the importance of this emerging technology. Along with the advancements in blockchain technology, smart contracts have shown great potential to affect the legal landscape. The legal profession should keep up with the technology process and examine its effects on legal studies and legal practice.

However, it is also immature to follow the trend without prudent thoughts and investigations. For example, a prevalent trend by some technology enthusiasts is claiming that smart contracts are likely to replace traditional legal contracts and could displace millions of legal jobs. A radical change has been sweeping the globe and smart contracts would overturn the legal industry with an unanticipated speed. Such rhetoric gives fresh urgency to the fear of the legal profession being displaced.

Therefore, it is critical to first identify the role of smart contracts in the current legal system and explore mechanisms for smart contracts to better serve the legal research, legal practice, legal professionals, and humanity, not to displace the legal industry thoroughly. In this article, the author proposes that smart contracts assume an instrumental role aimed at serving the current contract law system, instead of trying to become an alternative to that system. Embedding smart contracts within the current contract law system, which they function as a tool, represents a situation with considerable more potential for success. The success would derive from smart contracts' value of increased efficiency. With such value, the author further proposes three guidelines for enhanced instrumental functionality within the existing contract law system from three perspectives, including specification of areas of application, technological improvement, and legal support.

The Normative Role of Smart Contracts: The Smart Contract as Instrument

Smart contracts, in nature, are computer codes that run on blockchains (CoinDesk, 2016). However, some confuse it with traditional legal contracts which require a set of offer, acceptance, and consideration. The danger of mixing smart contracts and traditional legal contracts is raising unanticipated issues unsolvable by either legal professions or technicians.

The author recommend assigning an instrumental role to smart contracts, because distinguishing the role of smart contracts from that of traditional contracts within the contract law system could facilitate each one's ability to focus on its respective tasks, thereby strengthening the value of its role. The approach would situate smart contracts to pursue a course that runs parallel to that of traditional contract law: To wit, smart contracts can assume responsibility for the technical execution of contractual terms that do not have legal implications, while traditional contract law should concentrate on directing all actions related to the pertinent legal issues.

For example, imposing a practical distinction between the role of smart contracts and that of contract law would be able to furnish a solution to an issue of breach. An issue of breach reflects a dilemma between smart contracts and traditional legal contracts. Smart contracts intrinsically assume the absence of any breach throughout the contract performance phase, because putting smart contracts "on" the blockchain ensures that neither party has the capability in influence or interfere with its operation, the logical conclusion of which is a technical guarantee of contractual performance (Raskin, 2017). However, the dilemma is that smart contracts are hardly qualified to make such a guarantee, given that the possibility of failure to perform and satisfy contractual obligations simply originates from a different source, such as a potential bug in the code. Such a possibility is simply not on the spectrum of a smart contract's pre-defined outcomes. As such, a smart contract is treated as an isolated system, and the non-breached party has no way of obtaining remedies.

Under the contract law theory, this represents a breach, because the other party has failed to honor the exchange for which both parties bargained. If the smart contract is regarded as a tool, selected by contractual parties to execute their obligations, the failure of the tool to carry out its expected contractual obligations produces a situation wherein the non-breached party is entitled to remedies. Therefore, separating roles of smart contracts and traditional legal contracts bridges a gap between unsolvable issues by either legal or technical professions.

The Instrumental Value of Smart Contracts: Increased Efficiency

From an economic perspective, contract law's primary purpose is to maximize value, and the means to maximize value are through transactions (CoinDesk, 2016). The transaction is a core element of the economies of exchange. The standard economic assumption is that people are rational maximizers, seeking to maximize their value. Value is determined by the free preferences of individuals (Bayles, 1983). Therefore, if two people voluntarily arrange to exchange, e.g., money for goods, then both individuals' preferences will be satisfied. The satisfaction of their preferences increases value because both get something more valuable to them. Overall, welfare can be derived from those exchanges of resources. Voluntary transactions are the building blocks of the market; and a free and competitive market is the ideal prototype of an economically efficient mechanism (Zamir & Medina, 2010). Market transactions are not only Kaldor-Hicks efficient but also Pareto efficient because presumably no one would enter into a contract unless he or she expects it to improve his or her lot (Zamir & Medina, 2010).

The role of contract law is to facilitate and encourage those transactions for the purpose of value maximization. Contract law should provide the parties with optimal incentives to act efficiently, that is, in a way that would maximize the joint surplus from the transaction, throughout the contractual process (Zamir & Medina, 2010). Chronologically, this process begins by acquiring relevant information and searching for an appropriate partner, and it continues in negotiation and formulation of the contract, moving on to investment in performance efforts by the promisor and in reliance by the promise, deciding whether to perform or breach, and finally, taking measures in response to a possible breach (Zamir & Medina, 2010).

In contrast, on their own, smart contracts can neither facilitate nor encourage a voluntary exchange of resources, and thereby cannot replace the role of contract law in maximizing value. Smart contracts suffer from such deficiencies largely because of their procedural defects derived from the lack of pre-contractual phases. The phases that involve such tasks as the acquisition of information, the identification of partners, and the negotiation of contractual terms, all of which facilitate appropriate allocation of resources and risk assessment for value maximization purposes. However, if smart contracts exist not in isolation, but rather as component parts of the contract law system, then smart contracts can operate in concert with contract law rules to maximize value.

If we regard smart contracts as a tool embedded within the contract law system, and if in the performance of that instrumental role, smart contracts increase in value while contract law maintains its traditional roles and functions—engaging in pre-contractual phases, allocating recourses, assessing risks, and filling gaps—then this should work to maximize the overall value of the contract law system. As such, the intrinsic purpose of maximizing value dictates that the goal of the smart contract is to increase its instrumental value, which can occur in various ways.

One possible mode of increasing value would emerge from the reduced costs associated with the time required to draft and negotiate contracts. Smart contracts can be generated automatically via a platform, according to a predetermined pattern and syntax, thereby negating the need to craft a contract from scratch (Dewey, 2016). Such automation represents a tremendous increase in transactional efficiency, potentially applicable to many routine legal documents that could be created with minimal to no human involvement (Dewey, 2016). Further, since contract terms chosen should be clear enough to be encoded into the computer program, the charity, particularly with regard to terminology, minimizes the likelihood of over-interpretation, as well as the possibility of future litigations.

A second source of increased value derived from the relative speed of automated performance. Certain types of contracts operate in accordance with simple logic, enabling the fulfillment of contractual obligations with virtually equal facility by human or computer. For example, if X happens (i.e., T transfers the monthly rent of $1,000 to L), then Y follows (i.e., L transfers the digital key of his house to T). The obligations involved with providing the rent the digital key could be fulfilled with equal proficiency by human or smart contracts, voiding the physical tasks of transferring the rent and handing over the key, which would definitely represent savings in both time and money for both parties, thereby increasing efficiency.

A third variable associated with the smart contract's increased value is related to the ability to encode regulatory and other compliance logic into the platform (Dewey, 2016). Such coding would be likely to reduce, or even eliminate high costs, delays, and errors that demand personal handling or reworking in the context of highly-regulated industries, such as the financial industry or securities sector. For instance, due to their immutability feature, blockchain-based smart contracts maintain a record of compliance-related steps and processes required by regulatory agencies. A series of recording actions and their outputs form an audit trail, which is easily verifiable by any interested regulator or regulatory body. This automated procedure would represent a substantial conservation of the time and effort that financial institutions spend generating regulatory report, along with the effort associated with attempting to improve the accuracy and quality of the reporting process itself.

Fourth, smart contract value is maximized by enabling discontinued reliance on a third party. The intermediary cost tends to be a high and unavoidable one in the economic world. For instance, Alibaba, a Chinese e-commerce giant, offers an escrow service, Alipay, for the sake of conducting secure online payments. Alipay functions as an escrow holder for the purposes of heightening the security of transactions between a buyer and a seller. Alipay will not release the funds to the seller until or unless the buyer has received the goods purchased. Not only is this a time-consuming process, but Alipay requires additional escrow fees that increase expenditures associated with the transaction. Smart contracts have the potential to solve this trusted-related issue by using code to execute contractual terms automatically. In the case of a failure to deliver on the part of the seller, the buyer keeps the funds. This also occurs when the reverse scenario arises. Smart contracts guarantee that each side enjoys the protection of the agreement, and do so in the absence of additional expenditures associated with the cost of a trusted third party.

Guidelines for Enhanced Instrumental Functionality Within the Existing Contract Law System

Specification of Areas of Application

As indicated above, the first directive requires the specification of areas of application. Distinguishing between what smart contracts can do and cannot do is the primary task involved here, because smart contracts are not applicable to many areas of life. For example, when certain service contracts require contractors to supply time, effort, and expertise, smart contracts would not be able to fulfill such obligations, including cleaning houses, babysitting, or teaching in a school. But smart contracts probably operate more effectively than humans do in other areas, such as automating mundane and repetitive work, transmitting payments, and issuing certificates. For some industries, such as the financial sectors and supply chain industry, the application of smart contracts is likely to emerge and develop sooner than in many other industries. Therefore, determining the capability of smart contracts is the first step toward conclusively determining their value.

The next task involves distinguishing between efficient and inefficient uses of smart contracts to design a regime aimed at enhancing their efficacy. The use of smart contacts has been proposed in various industries, including finance, law, supply chain management, real estate, and the Internet of Things, as well as predictive and commodity markets. However, smart contract development is still in its infant stages. Most use cases cannot be realized for multiple reasons; some use cases are feasible but very costly, which is contrary to smart contracts' cost-saving goal, and a very limited number of use cases can be optimized to operate more efficiently than they do under the current paradigm. Therefore, the quest for efficient use cases is a significant component in the general enterprise of maximizing value.

Another important task involves that avoidance of new inefficiency. This is the task immediately follows our classification of efficient uses of smart contracts relative to current uses. New uses are likely to generate new inefficiencies that do not characterize the current uses. Such novel inefficiencies could result from the mechanical issues associated with the application of smart contracts, as well as non-mechanical reasons. For example, it is generally cost- and time- effective to employ smart contracts in real estate title transfers. However, replacing the current title transferal system requires corresponding adaption to legislation and law enforcement, which involve expenditures related to the adopting the system and training employees, as well as high maintenance fees. Such costs overwhelmingly surpass the benefits of applying smart contracts to real estate title transfers, thereby creating new inefficiencies. Non-mechanical reasons, such as the willingness of business owners to apply smart contracts, can also produce new inefficiencies. Although smart contracts may save tremendous amounts of time and money in the course of doing everyday business, stakeholders may be unlikely to transfer their valuable business without meaningful assurance that it will not demand a sacrifice of the hard-won legal rights they currently enjoy in exchange for nothing more than the efficiency of a smart contract. Therefore, balancing costs with benefits accounting for the issue of new inefficiencies is critical to maximize the value of smart contracts in specified areas and industries.

Technological Improvement

Threat prevention. Smart contracts remain highly experimental. The development of increasingly smart contract applications may yield new bugs and security risks. Call depth attacks, reentrance attacks, over- and under- flows, replay attacks, reordering attacks, and short address attacks are examples of several known bugs. It is challenging to avoid all attacks that might emerge during attempts to write the smart contracts. Despite of taking sufficient precautions in the first stage, attacks retain the potential to evolve during, or even after, a transaction. It is therefore critical to identify smart contracts' security vulnerabilities and generalize common programming traps that result in vulnerabilities associated with each program process.

Using the example of Ethereum smart contracts, it is possible to catalogue three classes of vulnerabilities, in accordance with the level at which they are introduced (Solidity, EVM bytecode, or blockchain) (Atzei, Bartoletti, & Cimoli, 2016). Some recent works propose tools to detect vulnerabilities via static analysis of the contract code (Atzei et al., 2016). For instance, the tool Oyente extracts the control flow graphs from the EVM bytecode of a contract, and symbolically executes them to detect any vulnerability patterns, particularly patterns that potentially lead to "exception disorder", "time constraints", "unpredictable state", and "reentrance" (Atzei et al., 2016). The result reflects the prevalence of security vulnerabilities that require developers to adopt their actions to respond.

Beyond inventing tools for spotting vulnerabilities in smart contracts, designers must take more general precautions as they progress. For example, smart contract designers should ensure the simplicity of the logic of their smart contracts, because logical complexity amplifies the opportunity for errors to emerge. Smart contracts engineers should conduct multiple tests before they finally execute the smart contracts. Upon detecting a threat, engineers should be able to eradicate it before a full production release. During the execution of smart contract, engineers should either manage to execute smart contracts safely, or be prepared to decisively suspend the process if any attack appears. Suspending the process is a judicious approach to managing loss if anything goes awry. After successful execution of a smart contract, designers or engineers should stay abreast of smart contract maintenance to prevent potential attacks.

Privacy protection. A lack of privacy is a mainhurdle impeding the widespread adoption of smart contracts, especially in financial and business industries. The solutions aimed at protecting privacy are in some cases feasible, and in some cases, compatible with the existing blockchain; the results, however, are not particularly satisfying (Burterin, 2016). Three solutions may reduce the lack of privacy: choosing between transparency and privacy, applying zero-knowledge proofs, and building privacy-preserving smart contracts. It is worth nothing that all of these present partial solutions designed to invoke privacy for specific classes of applications and are thereby incapable of addressing all privacy issues across all smart contract applications.

The first is considering the choice between transparency and privacy (Drescher, 2017). Achieving total privacy without compromising transparency is an unlikely pursuit. The primary goal here involves making a choice that most effectively meets the greatest need. This binary selection may lead to a choice between public and private blockchains. If the business or industry assigns a high value to privacy, then a private blockchain may be more suitable for running the smart contracts. A private blockchain can secure privacy by granting access to a limited number of participants in the network. If transparency is valued over privacy, then a public blockchain is probably the right choice, as it enables people to participate in verifying ownership and transactions in the smart contracts.

The second is considering the application of zero-knowledge proofs. "Zero-knowledge proofs allow one party (the prover) to prove to another (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself".[2] Zerocash exemplifies the application of technology that relies on zero-knowledge proof technology. For example, in the Bitcoin network, transactions are not confidential and the addresses are not free from identification. Zerocash enables users to avoid revealing the information of origin, destination, and the payment by adding privacy-preserving protocols. Such privacy-preserving protocols can, therefore, be applied to the public network for purposes of protecting privacy.

[2] Zcash, What are zk-SNARKs?, https://z.cash/technology/zksnarks.html (last visited March 27, 2018).

The third is considering the possibility of building privacy-preserving smart contracts. A criticism leveled at Zerocash is that the system is required to sacrifice programmability in exchange for privacy, and it remains unclear a priori how to facilitate programmability without exposing the clear text of transactions and data to miners (Kosba, Miller, Shi, Wen, & Papamanthou, 2016). Therefore, developers proposed Hawk, a novel framework for building privacy-preserving smart contracts. Hawk allows a non-specialist programmer to write a Hawk program that does not require the implementation of any form of cryptography (Kosba et al., 2016). Hawk can guarantee privacy through on-chain privacy and contractual security: While on-chain privacy protects contractual parties from public view via the use of encrypted information, contractual security protects parties within the same transaction from each other by preventing cheating and aborting behavior.

Overall, each of the above mentioned solutions yields increasingly tremendous value to the enterprise of protecting privacy, but they are (as a group) neither perfect nor free of limitations. Most iterations of these solutions are category- or case- based partial solutions. These solutions may also result in high transaction fees or high latency. It remains for us to go keep advancing to overcome more challenges.

Scalability enhancement. An inherent conflict exists between on the one hand, securing a transaction's history based on a time-consuming proof of work, and on the other, the required speed and scalability characteristic of many applications in commercial or financial contexts. The user must decide in the first place, between security and the most suitable speed scalability for the business or use (Drescher, 2017). Other solutions have been proposed to achieve different purposes: Segwit, block size increase, Plasma, etc.

First, analogous to the privacy issue, there is another unavoidable trade-off related to scalability. Obtaining absolute security is unlikely without compromising the scalability. This also leads to a choice between permissionless and permissioned blockchains. Choosing a permissionless blockchain indicates that the business or the industry places a greater emphasis on the accuracy and security of the transaction data by requiring the proof of work, even if this choice results in low transaction throughput. Choosing a permissioned blockchain indicates that higher transaction throughput is of particularly high value for the business or the industry, and it is thereby rational to sacrifice, at least to some extent, the benefit of a decentralized structure to achieve that throughput level.

There are two Bitcoin-specific solutions known as the 2-megabyte size increase and SegWit respectively. The 2-megabyte size increase refers to an increase in the current hard limit from 1 MB to 2 MB, thereby enables the network to manage more transactions per second in each block. The increase, however, raises a concern associated with splitting Bitcoin into separate payment networks.

Segregated Witness, known as SegWit, is a protocol upgrade that revolutionizes the way data are gathered and stored. It enhances the scalability by removing 60% of the transaction information and storing it outside the base transaction block (Kasireddy, 2017). The benefit that results from the removal of such information is increased space to hold data in each block containing SegWit transactions. The data limit in each block will increase from the 1 MB to a little less than 4 MB, providing an approximate 70% increase in transactions (Kasireddy, 2017). However, a controversy related to the implementation of SegWit involves the possibility that miners may earn fewer transaction fees for each transaction. Another challenge is related to the fact that all the wallets are required to implement SegWit before it is possible to enjoy its advantages, but the implementation process is a complex enough to generate the potential for mistakes. More importantly, the information that has been moved to the sidechain should also be maintained by miners too, but they have no financial incentive to do so.

Additionally, Plasma is

> a proposed framework for incentivized and enforced the execution of smart contracts which is scalable to a significant amount of state updates per second (potentially billions) enabling the blockchain to be able to represent a significant amount of decentralized financial applications worldwide. (Poon & Buterin, 2017)

Plasma enhances scalability via a series of contracts run on top of a root blockchain, such as the main Ethereum blockchain. The relationship between Ethereum and Plasma is akin to the relationship between the roots of a tree and its branches.[3] Branches can secure fault-free transactions through their own incentivized chain-validators. Only a portion of data will be submitted to the root for validation. This greatly reduces the burden on the root-main chain. Thus, Plasma can free a substantial amount of space in the main chain and also increase the transaction speed, thereby increasing the scalability of the smart contracts accordingly.

Law as the Pillar for Smart Contracts

Legislative clarifications to address controversies and new legal issues. The first step here requires invalidating the legal status of smart contracts. The law should clarify the legality of applying smart contracts to the automation of certain types and parts of legal contracts. In the same way that electronic documents are legalized and justified to serve as legal evidence in the context of judicial operations, smart contracts should be clarified and legalized as legal measures in the service of contract enforcement. Such legalization may avert legal challenges to the validity of applying the automation associated with smart contracts to a legal contract in the first place.

The law should also clarify the issue involved in controversial topics to pave the way for the widespread adoption of smart contracts. The best method for achieving this goal is to design smart contracts to run a parallel course to that of traditional contracts—smart contracts would be responsible for technical enforcement of contracts, but not authorized to handle any legal implications; all related legal issues should be guided by rules governing contract law. In other words, whenever parties sign a contract, they can choose whether to utilize or not to utilize smart contracts to fully or partially enforce contractual obligations. If they do choose to utilize smart contracts as the tool to execute the performance, contract law rules and theories serve to underpin the smart contracts, and as such, they guide, support, and govern the enforcement.

If that were the case, smart contracts would prompt less controversy related to issues of capacity, mutuality, and statutes of fraud of smart contracts. People cannot argue that they lack legal capacity when triggering the smart contract; they cannot recognize the meaning of the code, which obviates the potential occurrence of a meeting of the minds; and codes cannot be deemed as a “writing” in a way that satisfies the requirements of the Statute of Fraud, thereby rendering the contract unenforceable because all these legal issues would be resolved via contract law rules and theories. Smart contracts are merely a tool for enforcing legal contracts without additional legal implications.

Similarly, during the performance stage, rules and theories of contract law govern situations of part performance, impossibility or impracticability, and frustration of purposes. Additionally, while the enforcement involves in subjective judgment that smart contracts are incapable of justifying, there are two possible solutions to this deficit. One involves simply avoiding the use of smart contracts. The second indicates the viability of designing a mechanism to evaluate the level of discretion. For instance, in the case that “a contract for a

[3] Blockgeeks, Blockchain scalability: When, where, how? https://blockgeeks.com/guides/blockchain-scalability/ (last visited March 13, 2018).

painting is contingent on reasonable satisfaction of the potential buyer", the level of satisfaction can be scaled from one to five points. Once it reaches three points, it becomes reasonable, thereby triggering the smart contracts. For breach and remedies thereto, if smart contracts were to go amiss and execute an unexpected outcome, although smart contracts intrinsically assume a breach does not exist, this situation itself constitutes a breach under contract law theory. Remedies could follow according to the contract law rules as well. Therefore, once smart contracts and legal contracts coexist and are reasonable for disparate aspects, controversies can be addressed easily.

Besides that, legal guidance is needed in any situation where old questions confront new situations. For example, smart contracts raise important jurisdictional questions. Choice of law is a world in the process of adjusting to a new digital age. For instance, transactions that used to happen locally are rendered internationally because of the Internet. Such globalization raises a further question about which law prevails when the transactions extend across various countries or connect parties of diverse nationalities. Rules related to conflict of law afford clear guidance to applicable law. However, smart contracts, due to their distributed nature, add a new layer of complexity to the issues associated with choice of law. A transaction via the smart contract executes on every node across the network, which means the transaction occurs globally. All nodes (locations) appear to have the connection, and their respective courts might have jurisdiction, but this step is neither proper nor feasible. Therefore, clearer rules should be given with regard to the choice of law, to guarantee that the court will honor the choice of law chosen by the parties.

Legal standards for building a smart contract-based system. A common refrain concerning applications of smart contracts relates to a lack of legal standards governing those aiming to deploy a smart contract-based system. In every industry where smart contracts are applicable, legal standards for entry, process, and existence should exist. Otherwise, the applications will be chaotic.

First, it is necessary to standardize smart contract providers. There are many companies offering smart contract services. Issues of concern involve who is competent to provide services, whether the services provided are qualified, and how to evaluate the quality of the services. A series of industry standards should be articulated for guidance.

Second, it is further critical to establish standards governing the structure of smart contracts. In the world of legal contracts, the overall structures of contracts are similar and have become relatively standardized, although there might be some deviations according to various types of contracts. The structure of a contract usually starts by naming the parties to the contract, followed by the recitals, definitions, operative provisions, warranties and conditions, and miscellaneous clauses at the end. The commercial world greatly benefits from this implicit consensus on contractual structure. If smart contracts could attain a certain level of consensus with regard to structure, it would potentially ease the uses and widespread adoption of smart contracts.

Third, it would be extremely useful to standardize the execution of smart contracts, including how to translate legal prose into code, how to match pros and code correspondingly, and how to enforce contractual terms. These are very technical problems that, at the same time, require legal knowledge. A very challenging issue is a lack of experts who possess solid knowledge in both areas. Also, due to the fact that this is an early stage of the interplay between smart contracts and legal contracts, no clear consensus on terminologies is in use. A term often has divergent meanings between smart contract context and legal contract context, such as performance, breach, and enforcement. This ambiguity amplifies the difficulty of establishing a connection between smart contracts and legal contracts. It is therefore critical to the establishment of standards to avoid ambiguity and enhance the application of smart contracts.

Balancing regulations to shape the implementation of smart contracts. The implementation of smart contracts requires balanced regulation. Regulation is a double-edged sword; however, too much regulation can stifle innovation, while too little regulation may decrease confidence in the field or encourage illicit activities. The development of smart contracts is still in a very early stage, so regulators must stay abreast of the quickly-developing pace and react properly. The following three principles for regulations can shape a better implementation of smart contracts.

The fundamental task involves classifying regulations. Although it is unlikely that legislatures will regulate smart contracts as the technology in itself, the implementations of smart contracts in particular use cases may be the subject of additional regulatory scrutiny.[4] Also, certain cases are appropriate for regulation, while others are not. For example, the application of smart contracts to transactions that use cryptocurrencies as a method of payment or investment may be subject to financial regulation or securities regulation. Left totally unregulated, these activities may become a breeding ground for money laundering, fraud, and other illegal activities. On the other hand, for the implementation of smart contracts in government services to serve its citizens by issuing certificates, less regulation may be appropriate to reduce government expenditures, and increase efficiency of services. Therefore, it is critical to classify the necessity and levels of regulation appropriate in the various industries to avoid unnecessary interference and foster innovative environments.

Among all regulation techniques, technology is the key. Due to the nature of smart contracts, the current regulatory regime might not be suitable for new technological use cases. One possible answer here is to use technology to regulate technological use cases. For instance, a prevalent use case of current smart contracts is the transaction of cryptocurrencies. Regulators, using big data and cloud computing to search, collect, calculate, and analyze transaction data, detect and monitor high-frequency trading or irregular behaviors to further predict the legality of certain transactions. If a transaction is identified as illegal, it is suspended immediately for further investigation. This is how regulators use technology in a more real-time and effective manner than the traditional regulatory regime, such as ex-ante regulation (market entry approval) or ex-post regulation (punishment of the violation).

Moreover, the balance between innovation encouragement and risk prevention is important. A sandbox is a case in point. The word "sandbox" originally referred to a small box filled with sand where children could play and experiment in a controlled environment (BBVA News, 2017). In the digital era, the concept has referred to regulatory sandboxes, which are "testing grounds for new business models unprotected by current regulation or supervised by regulatory institutions" (BBVA News, 2017). Due to the nature of smart contracts, their application faces many uncertainties. The goal of regulation should be to encourage innovation and prevent risk. Regulatory sandboxes, by allowing innovators to test their products or business models in live environments without following legal requirements, have the potential to minimize legal uncertainty, improve access to investment, and generate rules for designing new products or business models. These goals are beneficial, especially to financial institutions and startup companies.

---

[4] Welcome to the future: Blockchain and the sharing economy, https://legalisglobal.com/welcome-to-the-future-blockchain-and-the-sharing-economy/ (last visited March 27, 2018).

Conclusion

Indeed, smart contracts could bring about the enormous impact to many industries that will revolutionize business and redefine economics. Therefore, it is critical to define the instrumental role of smart contracts and place them in the incumbent contract law. While sharing the enthusiasm for their great potential, we should also be aware that the transformation is decades away. Many issues should be addressed before their widespread adoption. Specifying areas of application, eliminating or reducing technological barriers, and having the law run as the pillar for smart contracts, are the key principles for smart contracts to better function as the tool of the existing contract law system. Through gradual experiments and further implementation, smart contracts are expected to seep into our business and economic infrastructure and make a difference. As legal scholars, we are the ones to bridge the gap between expectation and reality.

References

Atzei, N., Bartoletti, M., & Cimoli, T. (2016). *A survey of attacks on Ethereum smart contracts*. Retrieved Mar 13, 2018 from https://eprint.iacr.org/2016/1007.pdf

Bayles, M. D. (1983). Introduction: The purpose of contract law. *Valparaiso University Law Review, 17*(4), 613-626.

BBVA News. (2017). *What is a regulatory sandbox?* Retrieved March 27, 2018, from https://www.bbva.com/en/what-is-regulatory-sandbox/

Burterin, V. (2016). *Privacy on the blockchain: Ethereum blog*. Retrieved March 12, 2018, from https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

Coindesk. (2016). *Making sense of blockchain smart contracts*. Retrieved December 15, 2017, from https://www.coindesk.com/making-sense-smart-contracts/

Dewey, J. (2016). *What if we developed legal contracts like we developed software applications? Medium.* Retrieved March 27, 2018, from https://medium.com/@jndewey/what-if-we-developed-legal-contracts-like-we-developed-software-applications-6f8305256c5c

Drescher, D. (2017). *Blockchain basics: A non-technical introduction in 25 steps*. Retrieved March 26, 2018, from http//www.apress.com/la/book/9781484226032

Kasireddy, P. (2017). *Blockchains don't scale: Not today, at least, but there's hope*. Retrieved March 13, 2018, from https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 839-858). May 22-26, San Jose, USA.

Poon, J., & Buterin, V. (2017). *Plasma: Scalable autonomous smart contracts.* Retrieved March 13, 2018 from http://plasma.io/plasma.pdf

Raskin, M. (2017). *The law and legality of smart contracts*. Retrieved March 26, 2018, from https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/

Szabo, N. (1995). *Smart contracts glossary*. Retrieved December 12, 2017, from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_glossary.html

Zamir, E., & Medina, B. (2010). *Law, economics, and morality*. Oxford, New York: Oxford University Press. Retrieved March 5, 2018, from http://discovere.emory.edu/primo_library/libweb/action/dlDisplay.do?vid=discovere&afterPDS=true&docId=01EMORY_ALMA21241699040002486