SMART CONTRACTS: Is the Law Ready?

CHAMBER OF DIGITAL COMMERCE

SMART CONTRACTS ALLIANCE

PREPARED BY: SMART CONTRACTS ALLIANCE
AN INITIATIVE OF THE CHAMBER OF DIGITAL COMMERCE

SEPTEMBER 2018

ABOUT THE CHAMBER OF DIGITAL COMMERCE

The Chamber of Digital Commerce is the world's largest trade association representing the digital asset and blockchain industry. Our mission is to promote the acceptance and use of digital assets and blockchain technology. Through education, advocacy, and working closely with policy makers, regulatory agencies, and the blockchain industry, our goal is to develop a pro-growth legal environment that fosters innovation, jobs, and investment.

SMART CONTRACTS ALLIANCE

The Smart Contracts Alliance is an initiative of the Chamber of Digital Commerce to promote the acceptance and use of smart contract technologies to enhance the way business is conducted. Comprised of thought leaders and innovators from across the technology, legal, and financial services industries, the Smart Contracts Alliance is shaping how smart contracts are understood, developed, and adopted.

CHAMBER OF DIGITAL COMMERCE INDUSTRY INITIATIVES & WORKING GROUPS

TOKEN ALLIANCE

Fostering best practices and frameworks for the responsible growth of tokenized networks and applications, and fundraising through initial coin offerings.

BLOCKCHAIN INTELLECTUAL PROPERTY COUNCIL

Balancing the protection of proprietary information with the openness necessary for innovation.

DIGITAL ASSETS ACCOUNTING CONSORTIUM

Developing accounting and reporting standards for digital assets and blockchain technology.

GLOBAL BLOCKCHAIN FORUM

Working with the world's leading blockchain policy experts to develop industry best practices and help shape global regulatory interoperability.

BLOCKCHAIN ALLIANCE

The public-private forum for the blockchain community and law enforcement to help combat criminal activity.

STATE WORKING GROUP

Engaging with state and local governments on the regulation and implementation of blockchain technology.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The Chamber of Digital Commerce would like to recognize the following individuals for their thought leadership, contributions and support to the Smart Contracts Alliance in the production of this report.

SMART CONTRACTS ALLIANCE CO-CHAIRS

JORDAN EARLS

Lead Develper, QTUM

MARK SMITH

CEO, Symbiont

RONALD SMITH

Partner, Norton Rose Fulbright

KEY CONTRIBUTORS

MIREN APARICIO BIJUESCA

FinTech Lawyer and Senior Consultant, The World Bank

JOSHUA BOEHM

Associate, Perkins Coie

JENNY CIEPLAK

Counsel, Crowell & Moring

FRED FEDYNYSHYN

Senior Counsel, Perkins Coie

PATRICIA FRY

Professor of Law Emeritus, University of Missouri-Columbia School of Law

PHILLIP H. GRIFFIN

VP, EISA System Architect, Wells Fargo

DAX HANSEN

Partner, Perkins Coie

AMY DAVINE KIM

Chief Policy Officer, Chamber of Digital Commerce

SEAN MURPHY

Partner, Norton Rose Fulbright

MARK RADCLIFFE

Partner, DLA Piper

MARGO TANK

Partner, DLA Piper

DAVID WHITAKER

Partner, DLA Piper

SPECIAL ADVISORS

CAROLINA ABENANTE

Founder, Executive Vice-Chairperson, CSO and General Counsel, NYIAX

JAMES ANGEL

Associate Professor of Finance, McDonough School of Business, Georgetown University Center for Financial Markets and Policy

MIKE BELSHE

CEO, BitGo

LEWIS COHEN

Partner, DLx Law LLP

JOSHUA STEIN

CEO, Harbor

MICHAEL HANSEN

Head of Innovation, Discover Financial Services

CRAIG HAJDUK

Principal Product Manager, Blockchain Engineering, Microsoft

ROSARIO INGARGIOLA

Founder & CEO, OTCXN

JOHNATHAN JOHNSON

President, Medici Ventures

RAJ KARKARA

Senior Vice President, Advisory & Partnerships, tZERO

JACK LEE

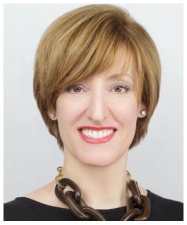
HCM Capital, Founding Managing Partner, Foxconn Technology Group

BRADFORD LEVY

Global Head Loans and CEO of MarkitSERV, IHS Markit

BYUNGKWON LIM

Partner, Debevoise & Plimpton



CAITLIN LONG

Co-Founder, Wyoming Blockchain Coalition

ERICK MILLER

Founder & CEO, Coin Circle

ANOOP NANNRA

Senior Leader & Head of Blockchain/DLT Initiative, Cisco Systems

GIRISH RAMACHANDRA

Senior Manager, Wipfli

JOE ROETS

Chief Architect, Founder, CEO, Dragonchain

MATTHEW ROSZAK

Chairman and Co-Founder, Bloq

PAUL SNOW

CEO, Factom

COLLEEN SULLIVAN

Partner & CEO, CMT Digital

MICAH WINKELSPECHT

Founder & CEO, Gem

JULIE WINKLER

CCO, CME Group

FOREWORD

By Mark Smith, CEO, Symbiont; Ronald Smith, Partner, Norton Rose Fulbright; and Jordan Earls, Lead Developer, QTUM

Smart contracts have come a long way in a short time. They will help to realize the many possibilities of distributed ledger technology (DLT). Certainty of outcome, automation of performance, and efficiencies in the streamlining of processes are reasons enough for smart contracts to be fundamental to the uptake of DLT. Their potential is now being actively considered and developed in sectors as diverse as Financial Services, Life Sciences and Healthcare, Technology and Telecoms, Transport, Energy, Infrastructure, Mining and Commodities. In Financial Services, for example, no one will be surprised to see smart contracts being used in areas such as securities clearing and settlement, collateral management, derivatives contracts, securities asset servicing, international money transfers, and perhaps even syndicated lending.

For many sectors it is the ability of smart contracts to be transformative in relation to existing business processes that is compelling. For others it is the potential of smart contracts to reduce execution risk (by making transfer of the relevant asset or instrument in question near to inevitable by virtue of automatic performance). As Chapter 3 of this white paper discusses, that may only achieve factual (that is, *de facto*) transfer. It may still be necessary, therefore, to apply established legal concepts and principles in order to determine whether transfer has been achieved at law (*de jure*).

Whether that is the case may turn in part on whether a smart contract has legally binding contractual effect in the first place. That is why this white paper, produced by the Smart Contracts Alliance, is so important. It will help those working in the smart contracts and DLT arena to “speak the same language” as their legal counsel when discussion turns to the legal effect of a smart contract: When can it be a legally binding contract? Does its electronic nature deprive it of contractual effect? Is it a security? Can it transfer assets or perfect a transfer of title to them? These are questions of fundamental importance, and will affect the extent to which smart contracts will be deployed beyond a role confined to self-executing, automating code.

Discussion within the smart contracts and DLT industry has come a long way from the time when smart contracts were often assumed to be contractual in effect – they are called contracts, after all, so why wouldn’t they have contractual effect? We know now that sometimes they may have contractual effect, and sometimes they will not. Importantly, this white paper makes clear that the difference between one and the other is not a strictly binary divide: a smart contract may affect legal relations (including contractual relations) between parties, even if the particular smart contract is not itself contractual, and a smart contract may also give rise to liabilities beyond breach of contract.

Legal clarity in relation to smart contracts is important because of other unrelated technology developments too. This white paper explains that, under legislation of some jurisdictions, smart contracts are likely to be regarded as “electronic agents,” with enabling consequences in terms of legal or contractual effect. Where might we see the deployment of electronic agents? Artificial Intelligence (AI) is, at the moment, probably the most talked about developing technology. Put AI machine learning in combination with electronic agents such as smart contracts and you have functionality that can autonomously decide and then automatically perform, without the need for human intervention. Realizing business efficiencies, transforming business processes, enabling peer-to-peer interactions, and de-risking aspects of established commercial transactions — the potential of smart contracts is enormous.

INTRODUCTION

In July 2016, the Chamber of Digital Commerce (the "Chamber") launched the Smart Contracts Alliance (the "SCA") to promote the acceptance and use of smart contract technologies to enhance the way business is conducted across industries. The SCA brings together thought leaders and innovators from across technology, legal, and financial services industries to help educate, collaborate, and shape policy for smart contracts moving forward. This effort allows the Chamber and the SCA to pool the collective knowledge of industry participants and form a broad-based understanding of the nature of smart contracts, their potential application, and how smart contracts fit into existing legal regimes. This SCA white paper (the "white paper") seeks to share the insights gained from the SCA's efforts and, in particular, from the work of the white paper's authors.

Although the term "smart contract" immediately pushes lawyers to questions of contract law, the reality is that smart contracts may be neither particularly smart, nor automatically intended to be used as a contract, in the legal sense of the word. In the SCA's view, a smart contract (in the context of blockchain technology) can be defined as follows:[1]

SMART CONTRACT

Computer code that, upon the occurance of a specified condition or conditions, is capable of running automatically according to prespecified functions. The code can be stored and processed on a distributed ledger and would write any resulting change into the distributed ledger.

Critical to this definition is the recognition that a smart contract is not necessarily a legal contract. Instead, a smart contract is essentially an advanced form of a conditional "if-then" statement written in computer code.

This white paper is organized into three chapters. The body of the white paper is comprised of the following chapters: (1) Formation, Modification, and Enforcement of Smart Legal Contracts; (2) Smart Contracts and Electronic Signatures and Records; (3) U.C.C. and State Law Issues in Smart Contracts.

[1] The SCA recognizes that term "smart contract" generally need not utilize a blockchain. Indeed, the original illustration of a smart contract, given by computer scientist Nick Szabo, was simply a vending machine that dispenses goods upon payment of a specified sum. However, for the purposes of this whitepaper, we use the term in the context of distributed ledger technology.

- The first chapter addresses the formation and enforcement of legal contracts using smart contracts, and it considers the various complications that may arise in the context of blockchains (*e.g.*, identification of parties, modification of terms, choice of law, enforcement, liability, etc.). The chapter considers law in both the United States and in Spain, which uses civil law, offering insight into how jurisdictional issues may impact digital platforms that span the globe.
- The second chapter addresses legal contracts that are implemented in whole or in part on a blockchain, and whether or not their use of a blockchain renders them enforceable under existing law. The chapter concludes that the Uniform Electronic Signatures Act ("UETA") and Electronic Signatures in Global and National Commerce Act ("ESIGN") already recognize, enable, and validate the use of electronic signatures and electronic records when using a blockchain.[2]
- The third chapter addresses smart contracts in the context of Article 9 of the Uniform Commercial Code ("U.C.C."). Specifically, this chapter explores issues surrounding the perfection of a security interest on the blockchain. This issue is hugely significant if parties to a contract wish to incorporate blockchain-based assets directly into their smart legal contracts.

It also includes a lexicon of blockchain-related terms. The lexicon—a key component of the white paper—provides a common point of understanding in a developing ecosystem that lacks a standard set of definitions. This definitional issue is critically important, as the meaning of a certain term in common use may vary depending on context and the profession of the person using the term—*e.g.*, "smart contract," as discussed above. The definitions in the lexicon serve principally to offer a common basis for understanding the analysis in this white paper. For that reason, the definitions reasonably may be applied elsewhere, as they were formulated with broad input from industry participants and following a review of definitions used in other writings.

The Chamber presents this white paper as a resource to industry, government, and the public. The SCA will continue to expand its knowledge on issues relating to smart contracts and promote smart contracts through its education and advocacy efforts.

[2] The timing of this white paper is critical for the development and adoption of smart contracts moving forward. In the opening months of 2018, a number of states introduced blockchain-related legislation. Many of these proposed laws seek to recognize legal agreements or terms that are implemented, formed, or executed on blockchains and, in so doing, offer definitions of "smart contract." These laws, while well-intentioned, in many cases are redundant to existing law, are inconsistently drafted, face potential federal pre-emption challenges, and have the potential of harming the adoption of smart contracts. The Chamber has previously issued public statements addressing this concern.

LEXICON

Smart contract: Computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions. The code can be stored and processed on a distributed ledger and would write any resulting change into the distributed ledger.

Smart legal contract: A smart contract that articulates and is capable of self-executing, on a legally-enforceable basis, the terms of an agreement between two or more parties.

Distributed ledger: Computer software that employs a shared database architecture to maintain multiple, identical copies of an auditable, up-to-date distributed digital record of transactions or data.

Blockchain: A specific type of distributed ledger technology that organizes data into blocks that are "chained" together chronologically by a cryptographic hash function and confirmed by a consensus mechanism.

Public blockchain: A blockchain that allows anyone with the appropriate computing capability to submit messages for processing, be involved in the process of reaching consensus, or otherwise participate in the network. The Bitcoin blockchain is an example of a public blockchain.

Private blockchain: A blockchain whose participants are pre-selected or subject to gated entry based on satisfaction of certain requirements or on approval by an administrator.v

Blockchain-based asset: An asset that consists solely of a digital token on a blockchain.

Tokenized asset: An asset that consists of intangible or tangible property apart from a blockchain, such as real or chattel property or a legal interest in some asset, but which is represented by a token on a blockchain.

Virtual currency: A medium of exchange that operates like a currency in some environments, but that does not have all the attributes of fiat currency, in particular that does not have legal tender status in any jurisdiction.

Virtual currency wallet: A software application or other digital mechanism for holding, storing, and transferring a virtual currency.

Public/private key signature: A method of ensuring data integrity and origin authenticity that uses a party's private key to sign and its corresponding public key to verify the validity of its signature.

CHAPTER 1: THE CHALLENGES ASSOCIATED WITH SMART CONTRACTS: FORMATION, MODIFICATION, AND ENFORCEMENT

Miren B. Aparicio Bijuesca[3]

This chapter examines: 1) whether smart contracts can give rise to legally binding contracts; 2) a number of different models for smart contracts, when they might be appropriately used, and what factors might limit use (such as the need to amend or suspend performance); 3) the governing law applicable to smart contracts; 4) enforceability of smart contracts, limits to remedies available in court with respect to smart contracts, and alternative "self-help" mechanisms; and 5) finally, beyond issues of contractual liability, other non-contractual liabilities with respect to smart contracts. The answers vary depending on the model of the smart contract deployed and the law of the relevant jurisdiction.[4]

This chapter considers these questions from the standpoint of two different systems of law—United States common law and Spanish civil law—to demonstrate where there are likely to be common principles between disparate legal systems and where the answers are likely to diverge.[5]

I. CAN A SMART CONTRACT SATISFY THE ELEMENTS OF A CONTRACT?

To determine whether a smart contract can give rise to a legally enforceable contract, one must consider whether each of the elements necessary for a legally binding contract is met. Part 1 examines the elements of a legally binding contract under both U.S. and Spanish law.

[3] The author is thankful to Gonzalo Sánchez del Cura (Linklaters), Ricardo de Ángel Yágüez (Professor Emeritus at U. Deusto), Jenny Cieplak (Crowell & Moring), and Mark Radcliffe (DLA Piper) for their comments to this chapter. Thanks are also due Ronald Smith, Allison Gold, Jay Greathouse, Daniel Jackson, and Julia Massa (all from Norton Rose Fulbright US LLP) for their contributions to this chapter, particularly the sections regarding U.S. law.

[4] Computer scientists may be unaware of the legal consequences to the rights and duties of the parties that smart contracts produce. For instance, the Ethereum white paper states that its smart contracts "should not be seen as something that should be 'fulfilled' or 'complied with'; rather they are like 'autonomous agents' that live inside of the Ethereum execution environment." Vitalik Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, Github, (last visited May 24, 2018). However, as some authors note, even smart contracts in public blockchains may alter the future rights and obligations of the parties involved. *See* Kevin Werbach & Nicolas Cornell, Contracts Ex Machina, 67 Duke L.J. 313, 328-34 (2017).

[5] *Id.* at 353 ("Smart contracts could illuminate foundational issues in the theory of contracts.").

ELEMENTS OF A SMART CONTRACT

UNITED STATES	SPAIN
✓ OFFER	✓ CONSENT
✓ CONSENT	✓ OBJECT
✓ CONSIDERATION	✓ CAUSE
"To create a legally enforceable contract under U.S. law, two or more parties must demonstrate that an offer was made and accepted through a meeting of the minds, and accompanied by an exchange of consideration."	"Spanish Civil Code states that a contract 'exists when one or several persons agree to commit, mutually or reciprocally, to give something or do some service.'"

A. CAN A SMART CONTRACT SATISFY THE ELEMENTS OF A CONTRACT UNDER U.S. LAW?

To create a legally enforceable contract under U.S. law, two or more parties must generally demonstrate that an offer was made and accepted through a "meeting of the minds" and accompanied by an exchange of consideration. How such elements are satisfied varies according to the common law of each U.S. state. The sections immediately below consider whether a smart contract might satisfy each element and, by so doing, constitute a legally binding contract under U.S. law.[6]

1. OFFER

Generally speaking, under U.S. law "[a]n offer is an expression by one party of his assent to certain definite terms, provided that the other party involved in the bargaining transaction will likewise express his assent to the identically same terms."[7]

In many cases, smart contract code deployed on a distributed ledger would likely constitute an offer if other participants on the ledger are entitled to interact with and execute on the code. By way of example, in the well-established context of algorithmic trading, parties use computerized algorithms as "negotiators" before a contract is formed, allowing the parties to choose the order terms to offer to the market.[8] Counterparties, which may also be algorithmic traders, choose which terms they wish to accept. Further, in some distributed ledger systems, a party can send the terms of a proposed smart contract to another party, constituting an offer solely to the receiving party.

[6] The Restatement (Second) of Contracts defines a contract under U.S. law as "a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty." Restatement (Second) of Contracts § 1 (Am. Law. Inst. 1981).

[7] 1 Corbin on Contracts § 11, 23 (1963), as reprinted in Robert S. Summers & Robert A. Hillman, Contract and Related Obligation: Theory, Doctrine, and Practice, 403 (4th Ed. 2001).

[8] *See, e.g.*, Scholz, L., Algorithmic Contracts, 20 Stan. Tech. L. Rev. 128 (2017).

2. ACCEPTANCE

The second element of a legally enforceable contract under U.S. common law is acceptance of the offer by the counterparty.[9] Acceptance can be made either by formal acceptance (*i.e.*, by signature, making a return promise) or, under the right circumstances, by beginning or completing performance pursuant to terms of the offer.[10] In either case, acceptance requires both an agreement by the counterparty to the substantive terms of the contract and action by the counterparty to accept within the time period and by the procedure required by the offer.[11] Acceptance under U.S. law involves a "meeting of the minds." In other words, the parties need to have agreed to the same basic terms of the contract.[12]

In the case of a smart contract, the offeree (or, in the case of a smart contract simply posted on a public ledger, any participant in the ledger) may indicate acceptance through signing the transaction with a private key. Deploying a smart contract to a distributed ledger and signing the smart contract with a private key should constitute a valid offer and acceptance under applicable U.S. law if done correctly, as discussed in Chapter 2 below. Alternatively, parties may use computerized algorithms (or, conceivably, true AI, at some point in the future) to negotiate the terms of a smart contract. The algorithmic functioning or "decision-making" employed in such cases may, however, be complex, posing challenges to both courts and the parties themselves in the event of a contract dispute.[13]

Some commentators believe that parties to a smart contract can have a "meeting of the minds" under U.S. law when at least one side of the contracting process is consummated without human participation or intervention. This view is based on agency law principles and specific provisions in the federal Electronic Signatures in Global and National Commerce Act ("ESIGN Act") and the state Uniform Electronic Transactions Act of 1999 ("UETA"). Where contracts are entered into by an electronic agent (*i.e.*, software that has been programmed to act for and bind a principal), both the ESIGN Act and UETA attribute the computer's actions to the person or legal entity being bound.[14] The complexity of the electronic "minds" representing the parties is not explicitly a factor in these provisions.

3. CONSIDERATION

To be a legally binding contract under U.S. common law, the exchanged promises must be "bargained for." This means that each party must give some form of consideration to the other – a type of value must be exchanged.[15] Value can be given now or in the future and a promise to perform in the future constitutes valid consideration.

[9] *Id.* at 417.

[10] Restatement (Second) of Contracts, *supra* note 6 at § 32 ("In case of doubt an offer is interpreted as inviting the offeree to accept either by promising to perform what the offer requests or by rendering the performance, as the offeree chooses.").

[11] *See, e.g.*, U.C.C. § 2-206(1)(a)(1) ("Unless otherwise unambiguously indicated by the language or circumstances (a) an offer to make a contract shall be construed as inviting acceptance in any manner and by any medium reasonable in the circumstances.").

[12] Restatement (Second) of Contracts, *supra* note 6 at § 20.

[13] *See* Scholz, *supra* note 8.

[14] *See* Chapter 2, Part 3 *infra*. analysis on the electronic agent in US legislation, under the Electronic Signatures in Global and National Commerce Act ("ESIGN Act,") 15 U.S.C. § 7001 *et seq.* And the Uniform Electronic Transactions Act of 1999 ("UETA").

[15] Notably, the exchanged value need not be the exchange of equivalent value. *See* 1 J. Story, Commentaries on Equity Jurisprudence as Administered in England and America 337 (14th ed., 1918).

4. ANALYSIS OF SMART CONTRACTS UNDER THE THREE KEY ELEMENTS OF U.S. CONTRACT LAW

Although an initial question may simply be whether computer code is an adequate method for conveying the terms of an agreement, commentators agree that "mutual assent can take many forms, so long as it clearly implies agreement."[16] The more apt question, then, is whether smart contracts can meet the elements required of a legally enforceable agreement in the United States.

Smart contract code deployed on a distributed ledger can constitute an offer if any participant on the ledger is entitled to execute on the smart contract. In some distributed ledger systems, a party can send a smart contract to another party, constituting an offer solely to that other party. The offeree (or, in the case of a smart contract posted on a public ledger, any participant in the ledger) indicates acceptance through signing the transaction with the participants' private key. Deploying a smart contract to a distributed ledger, and signing a smart contract with a private key, constitutes valid offer and acceptance under applicable U.S. statutes, as discussed in Chapter 2 of this paper.

The use of smart contracts may raise questions about whether the contracting parties have had a "meeting of the minds," when at least one side of the contracting process is consummated without human participation or intervention. However, some authors have responded favorably to these questions based on agency law principles and specific provisions in the ESIGN Act and the UETA. Where contracts are entered into by an electronic agent (*i.e.*, software that has been programmed to act for and bind a principal), both the ESIGN Act and UETA attribute the computer's actions to the person or legal entity being bound.[17]

Parties to a smart legal contract should also be able to show consideration. Consideration can come in two forms—an exchange of value or performance at the outset of the contract, or a promise to perform or pay something of value in the future. Whether consideration exists is not a problem exclusive to smart contracts. For example, the conditional statement that "if it rains on Tuesday, Alice will give Bob $10" is not a contract unless Bob reciprocates consideration to Alice. The contract, whether a smart contract, smart legal contract, or otherwise, would need to reference some form of consideration.

Lack of consideration is not an issue that is inherent in smart contracts, however, because automated performance by both parties on the blockchain is not always possible. Even for smart contracts such as the smart contracts employed by the now-defunct Decentralized Autonomous Organization ("DAO"),[18] the parties who were responsible for curating the DAO investments needed to take actions offline to enter into investments for their fund and convert any gains

[16] Werbach & Cornell, *supra* note 5, at 342; *see also* Harry Surden, Computable Contracts, 46 U.C. Davis L. Rev. 629, 656 (2012) ("At a minimum, contract laws do not explicitly prohibit expressing contractual obligations in terms of data. More affirmatively, basic contracting principles actively accommodate data-oriented representation."); Jeremey M. Sklaroff, Comment, Smart Contracts and the Cost of Inflexibility, 166 U. Pa. L. Rev. 263, 286-291 (2017) (describing the evolution of EDI and its use in contracting and business processes).

[17] *See* Chapter 2, Part 3 *infra*. regarding analysis on the electronic agent in U.S. legislation, under the ESIGN Act and the UETA.

[18] *See* SEC, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Securities Act Release No. 81207 (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

into ether for distribution to the DAO participants. Nevertheless, this does not render the smart contract unenforceable since the promises made by the DAO curators would have (most likely) constituted sufficient consideration for a contract to exist.

The elements of contract formation in U.S. contract law can be satisfied by what is referred to as a "unilateral contract." In a unilateral contract, one party makes an offer, and the other party accepts it through its performance rather than through simply indicating consent.[19] Under certain circumstances, a smart contract might be construed as a unilateral contract offer.[20] For example, the act of depositing digital tokens into the DAO smart contract constituted acceptance of the related offer.

SMART CONTRACT DEPLOYMENT WILL CROSS BORDERS IN MANY CASES, REQUIRING A SEPARATE ANALYSIS OF CONTRACT LAW IN EACH RELEVANT JURISDICTION.

If each of the above elements—offer, acceptance, and consideration—is satisfied, a smart contract should be legally binding under U.S. law. However, the same result will not necessarily occur in other sovereign jurisdictions. Smart contract deployment will cross borders in many cases, requiring a separate analysis of contract law in each relevant jurisdiction. The following section examines the basic elements of contract law through the civil law lens of Spain, providing a useful point of comparison with the U.S. principles just discussed.

B. CAN A SMART CONTRACT SATISFY THE ELEMENTS OF A CONTRACT UNDER SPAIN'S CIVIL LAW?

Spain's Civil Code (the "Civil Code" or "C.c.")[21] states that "a contract exists when one or several persons agree to commit, mutually or reciprocally, to give something or do some service."[22] Certain elements must be satisfied for a smart contract to be legally binding under Spanish law: 1) consent through an offer and acceptance (similar to the "meeting of the minds" under U.S. law) by a person or entity with legal capacity to conclude the contract; 2) object of the obligation, which must be determined or determinable; and 3) cause of the obligation (similar to "consideration" under U.S. law).[23]

[19] I. Maurice Wormser, The True Conception of Unilateral Contracts, 26 Yale L.J. 136, 136 (1916).

[20] Werbach & Cornell, *supra* note 5, at 340-42.

[21] Codigo Civil ("C.c."), B.O.E. num. 206, July 25, 1889 (Spain), http://www.boe.es/buscar/pdf/1889/BOE-A-1889-4763-consolidado.pdf. *See* English version: http://www.wipo.int/wipolex/en/text.jsp?file_id=221319#LinkTarget_6407.

[22] Art. 1254 C.c. *See also* Luis Díez-Picazo and Antonio Gullón, 2 Sistema de Derecho Civil, 29-40 (Tecnos ed., 1976). The parties cannot agree on something prohibited or contrary to the law (Art. 1255 C.c.). The contract is the law between the parties or lex privata (Art. 1257 C.c.).

[23] Art. 1261 C.c. *See also* Articles 23 and 27 of the Law No. 34/2002 of July 11, 2002 on Information Society Services and Electronic Commerce (as last amended by Law No. 7/2010 of March 31, 2010, http://www.wipo.int/edocs/lexdocs/laws/es/es/es159es.pdf.

1. CONSENT

Valid consent means that the parties to the agreement (natural persons or legal entities) have legal capacity to enter into a contractual relationship. The Civil Code assumes legal capacity in all adults, unless a court declares them to be incapacitated by law.[24] For instance, there is no consent in the case of a minor or if entering into the contract was induced by mistake or by violence.[25]

A key issue in the case of consent under Spanish law is the question of the identity of the parties. Only natural or legal persons can be parties to a contract under Spanish law.[26] Thus, if the contracting parties cannot be identified, there is no valid declaration of consent, which is required for a contractual relationship to arise.[27] However, under Spanish law, a party may act pseudonymously but be identifiable when represented by an agent or proxy. The mandate can be express or verbal, but if verbal, the contracting party must ratify the agreement later.[28] Private blockchains, unlike public blockchains, probably fulfill the identification requirement needed for valid consent through the procedures that permit access to the platform. On the other hand, many smart contracts in public blockchains do not require identification of the participant. A participant may participate pseudonymously. Although this raises the problem of establishing valid consent, the problem could be addressed by the design of the blockchain (or its governance), which could provide for identification requirements. Similarly, the identity of a participant could be confirmed off-chain or be an integral part of the smart contract itself.

Consent based on performance, which is characteristic of some smart contracts, is a valid form of acceptance under Spain's civil law.[29] Initiating actions to execute an agreement shows that a party accepts its terms. For instance, ceding control of a private encryption key over a specified amount of digital tokens constitutes valid acceptance of an offer.[30]

Under Spanish law, valid consent to the precise terms of the offer is necessary. Acceptance must not be partial (or constitute a "counter-offer") but, rather, must refer to all the terms of the offer. The offer also must not have expired at the time consent is given.[31]

[24] Under certain circumstances, including temporary prohibitions, people cannot engage in particular contracts. For instance, the prohibitions of the official receivers to purchase any goods subject to a banckruptcy in art. 151 of the banckuptcy law (Ley 22/2003, de 9 de julio, Concursal).

[25] Article 1263 C.c. "The following persons cannot give their consent: Non-emancipated minors. Incapacitated persons."

[26] Similar to French law: "In a smart contract context, the main issue is not the legal capacity of the parties, but their identity. Blockchain transactions can be pseudonymous (as the use of a single public key only authenticates each participant to a blockchain without necessarily providing nor checking their identity). Trusted third party services are not required to participate in a blockchain transaction." *See* Norton Rose Fulbright, Can Smart Contracts Be Legally Binding Contracts, 41 (Nov. 2016), http://www.nortonrosefulbright.com/knowledge/publications/144559/can-smart-contracts-be-legally-binding-contracts.

[27] Díez-Picazo & Gullón, *supra* note 17 at 137. Art 1261 C.c.: "There is no contract unless the following requirements are present:Consent of the contracting parties.A certain object which is the subject matter of the agreement. Cause of the obligation established".

[28] Article 1710 C.c.. "The mandate may be express or implied. An express mandate may be executed pursuant to a public or private instrument, and even verbally. Acceptance may also be express or implied, as deduced from the acts of the attorney." *See also* Art. 1280 C.c.

[29] Max Raskin, The Law and Legality of Smart Contracts, 1 Geo. L. Tech. Rev. 304, 309-22 (2017). As the author notes, a common characteristic of smart contracts is that, "unlike traditional contracts acceptance comes through performance."

[30] Werbach & Cornell, *supra* note 4 at 53.

[31] Díez-Picazo & Gullón, *supra* note 17 at 75.

How might such requirements apply in the case of a smart contract? A smart contract can specify the timeframe required for acceptance, otherwise it may be assumed to be open for acceptance indefinitely. Moreover, because content placed on a blockchain is immutable (at least as the technology stands at the moment), it is not currently possible to alter the terms of an offer once it has been placed on a blockchain. Accordingly, the contract is executed when the offeree accepts the terms set in the code by performing certain actions. The parties would need to negotiate off-chain or encode a new smart contract in order to change the terms or the outcome of an existing smart contract (*see* Part 3 *infra*).

2. OBJECT

The Civil Code provides that the object, which is the subject matter of each party's obligation, needs to be: 1) determined or determinable at the time the contract is concluded; 2) lawful;[32] and 3) certain.

Space does not permit an analysis of all these requirements in relation to smart contracts. Probably the most salient requirement is that the object of a smart contract needs to be "certain." Some or all of the terms of a proposed agreement in natural language could be translated into code or coded in scripting language directly. In particular, using computer code could be advantageous when drafting certain operational clauses (for example, payment clauses) in legal agreements. Computer code is more limited than natural language, but it provides less room for ambiguity, so arguably "while computer code is subject to the same human error that written language is, it is much less subject to uncertainty."[33] Code-scripting language is a valid mechanism under Spanish law for defining the parties' rights and obligations, if such is the parties' intention.

3. CAUSE

The "cause" in Spanish civil law is a similar concept to "consideration" in U.S. law. The cause defines the actions of the parties and the reasons why they concluded an agreement. Under Spanish law, the cause is an essential element of a contract.[34] In a bilateral contract (*i.e.*, a contract under which both parties promise to perform an act in exchange for the other party's act), the cause of an obligation is linked to the other party's performance of its obligation. For example, payment might be linked to delivery.

4. ANALYSIS OF SMART CONTRACTS UNDER THE THREE KEY ELEMENTS OF SPAIN'S CONTRACT LAW

A smart legal contract can regulate the legal relationship between the parties when it integrates all the elements of a contract (consent, cause, and object). Specifically, the principle *pacta*

[32] *See* Articles 1261 C.c. and 1271 C.c. Goods or services that are not out of commerce and not contrary to law or morality can be the object of contracts.

[33] Raskin, *supra* note 24 at 324.

[34] Art.1275 C.c. "Contracts without cause or with unlawful cause shall have no effect whatsoever. The cause is unlawful when it is against the law or good morals." *See also* Supreme Court decisions of 8 July 1977, 1 April 1982, 30 December 1985.

sunt servanda ("pacts must be obeyed") summarizes in civil laws the effects of an agreement between the parties (*lex privata*). This is similar to contract law as a voluntary liability in common law doctrine in that contracts produce effects between the parties that create them.[35] The Civil Code specifically provides that "contracts are law between the parties to an agreement."[36]

The design of the blockchain and corresponding identification requirements have important consequences. Similar to the French Civil Code, parties to an agreement must be identifiable to provide a valid consent, which is an essential element of a contract.[37] Transactions on public blockchains may be highly decentralized due to the potentially unlimited number of participants and high number of parties verifying and processing the transactions, and digital identity does not necessarily correspond to a real identity (*i.e.*, identity documents issued by an official or governmental source).[38] However, the pseudo-anonymity feature in public blockchains can be changed by the design of the blockchain and replaced with identification requirements.[39] Self-regulatory frameworks may decide that the identities of participants in transactions on public or private blockchains (which are typically verified by a central party) could be verified off-chain.

The general rule is that the parties are free to choose the form for the acceptance of an offer. Smart legal contracts use software language applications on the blockchain rather than legal forms. Consent can be based on performance in the Civil Code (*i.e.*, transfer of cryptographic keys).[40] A smart legal contract may contain the terms of the agreement in natural language, which is translated into code or coded in scripting language directly. The code-scripting language is a valid mechanism under Spanish law to define the parties' rights and obligations if such is the parties' intention.

THE ELEMENTS OF A CONTRACT UNDER SPANISH LAW ARE SIMILAR TO THE ELEMENTS OF A CONTRACT UNDER U.S. LAW, THOUGH THE TERMINOLOGY IS DISTINCT.

In sum, a smart contract can also give rise to a legally binding contract under Spanish civil law. The elements of a contract under Spanish law are similar to the elements of a contract under

[35] Art. 1258 C.c. *See also* Werbach & Cornell, *supra* note 5 at 36-9.

[36] Art. 1091 C.c. and Article 1,278 C.c. "Contracts shall be binding, whatever the form under which they have been entered into, provided that they meet the essential conditions for their validity".

[37] *See* Norton Rose Fulbright, *supra* note 33 at 40-41

[38] High participation is what provides the benefit of trust based on maximum decentralization. In public blockchains, anyone can perform or verify transactions once they install the correct software. Trust is built by replacing intermediaries with user-driven consensus. *See* Sklaroff, *supra* note 19 at 277.

[39] Several self-regulatory initiatives explore frameworks where particpants are validated off-chain by a third party providing KYC/AML and investor accreditation due diligence to the participants in the network. *See* Maria A. Vidal, LegalBlock Activity 2: Transaction Permissionless Layer. A Framework for Self-Regulation, Medium (Apr. 22, 2018), https://medium.com/legal-block/legalblock-activity-2-ec5f86ee95e5.

[40] Werbach & Cornell, *supra* note 5 at 53.

U.S. law, though the terminology is distinct. Smart contract code is a valid mechanism to define the parties' contractual rights and obligations, should they choose to use it to do so.[41] The parties may act pseudonymously, but there must be a link (including off-chain) to their real identity to provide for valid consent, which is a crucial element of a contract under Spanish law.[42]

It is apparent from the foregoing that a smart contract could satisfy the requirements necessary for a legally binding contract to form under both U.S. law and under Spanish civil law. Whether that is so in a given case will depend on the parties' intentions, and the facts and the circumstances surrounding the particular smart contract deployed.

C. OTHER LAWS APPLICABLE TO SMART CONTRACTS

In addition to general laws that apply to determine whether a legally binding contract is formed as a matter of contract law, other more particular laws may apply to determine the issue in particular types of smart contract deployments, industries, or use cases. Space does not permit a detailed consideration of these (which will vary by jurisdiction), but examples include:

» "Business to customer" or "B2C" contracts under the European Union's consumer protection laws.[43]

» Under Spanish law, a consumer who has entered into an agreement that has been drafted by a commercial entity has the right to obtain the terms and conditions of a contract on paper at any time (failure to comply may nullify the contract that would otherwise have formed).[44]

» In the United States, the Statute of Frauds (a requirement deriving from English common law that certain types of contracts must be formalized in writing) may dictate whether particular smart contracts terms must be memorialized as opposed to strictly self-executing. For example, contracts that cannot be performed within one year are typically subject to the Statute of Frauds.

[41] Art. 1091 C.c. and Article 1,278 C.c. "Contracts shall be binding, whatever the form under which they have been entered into, provided that they meet the essential conditions for their validity."

[42] Art 1261 C.c. Several self-regulatory initiatives explore frameworks where particpants are validated off-chain by a third party and investor accreditation due diligence to the participants in the network.

[43] This paper does not address the E.U. General Data Protection Regulation ("GDPR"), which is an issue of some discussion in blockchain circles.

[44] Articles 7, 8 and 9 of Law 22/2007, Of July 11, On Distance Marketing Of Financial Services To Consumers, https://www.global-regulation.com/translation/spain/1445417/law-22-2007%252c-of-july-11%252c-on-distance-marketing-of-financial-services-to-consumers.html.
"Article 9. Communication of contractual terms and conditions and of the prior information.
1. the supplier shall inform consumer all conditions contract, as well as the information referred to in the preceding articles 7 and 8, on paper or another durable medium accessible to the consumer, in advance of the possible conclusion of the contract to distance or the acceptance of an offer and, in any case, until the consumer assumes obligations under any contract to distance or offer.

2. without prejudice to the fulfilment of the requirements of incorporation of the General contractual conditions, the supplier shall comply with the obligations laid down in paragraph 1, immediately after the conclusion of the contract when it was held at the request of the consumer using a technique of communication at a distance that does not allow transmit contractual terms and conditions and the information required pursuant to the provisions of said paragraph 1.

3. at any time the contractual relationship, consumer shall have the right, if you request, to obtain contractual terms and conditions on paper. In addition, the consumer shall have the right to change technique or techniques of distance communication used, unless it is incompatible with the contract concluded or the nature of the financial service provided.

4. the failure to comply with requirements relating to previous information arising from contracts, as well as relating to the communication of such prior information, is set out in Chapter II, in articles 7, 8 and 9 of this Act, may give rise to the nullity of contracts, in accordance with Spanish legislation."

Along the same lines, some types of contracts must comply with certain formalities in certain jurisdictions (such as requiring a notarial deed and registration or a medallion guarantee) for the contract to have effect vis-à-vis third parties. In Spain, for example, this includes the transfer of real estate titles, mortgages, and marriage documents.[45] Where registration formalities are required by Spanish law, a smart contract that might otherwise have legally binding effect between the parties would likely not be sufficient to transfer ownership in real property.

These examples underscore the need for advice regarding local law on any proposed smart contract to ensure that the deployment and smart contract model chosen meet local law requirements.

II. THE DIVIDING LINE: WHEN DO SMART CONTRACTS CONSTITUTE LEGALLY BINDING CONTRACTS?

Part 2 seeks to set out some common principles for smart contract developers to use in assessing whether their proposed smart contract model will give rise to legally binding contracts under the applicable legal system(s), if such is their intention.

A smart contract is simply computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions. It is not synonymous with a legally binding contract. Smart contracts can be (and are being) used in applications that have very little to do with acting as a legally binding contract (*e.g.*, supply chain management, self-sovereign identity, and provenance tracking). This does not mean that smart contracts can never constitute or form part of a legally binding contract. The discussion in Part 1 demonstrates that, under certain circumstances and if so decided by the parties, smart contracts can fulfill the elements of a legally binding contract under common law and civil law systems, such as the United States and Spain.

Moreover, legislation in some jurisdictions can help to support that outcome. For example:

- U.S. legislation such as the ESIGN Act and UETA, discussed in Chapter 2, may impact the analysis of whether any automated contract, including a smart contract, constitutes a legally binding contract.[46]
- Various U.S. state legislatures (*e.g.*, Arizona and Tennessee) have enacted or are planning to enact specific legislation attempting to authorize the use of smart contracts in electronic records and signatures, so that they are fully enforceable by a court of law.[47]
- Wyoming recently enacted a series of laws promoting the use of blockchain technology.[48] The legislation established a Blockchain Taskforce to further facilitate regulatory oversight of blockchain ventures within the state.

[45] Art. 1280 C.c. This list is not exhaustive (mortgages, marriage, wills, long term leasing agreements).
[46] Chapter 2, Part 3 *infra*.
[47] Arizona Rev. Stat. 44-7061 (2017).
[48] Wang, E., The State of Wyoming Charters Blockchain Technology, Lunar Digital Assets, May 31, 2018.

The analysis set out in Part 1 of U.S. and Spanish law supports the following general observations:

- The use of smart contracts or any automated contracts to support legally binding contracts does not in and of itself require enacting legislation, and it is supported by Spain's civil code and specific e-commerce legislation.[49]
- Subject to the bullet point immediately following below, the form in which a smart contract is expressed is not typically determinative of whether it gives rise to legally binding contractual relations. For example, in Spain, the code-scripting language would be a valid mechanism under Spanish contract law to define the parties' rights and obligations (*lex privata*), if such is the parties' intention. Similarly, under U.S. law, the form in which the contract is recorded is not typically determinative of whether a legally binding contract exists.[50]
- Contracts requiring adherence to particular legal formalities (for example, that the real estate transaction be embodied in a deed and registered) or dealing with consumers do not lend themselves to deployment within the smart contract context, unless other legal requirements are complied with.[51]
- Even if a smart contract deployment does not give rise to a legally binding contract, it may still affect legal relations between the parties (or with third parties in case of tort liability). Accordingly, those involved in smart contract deployments should still consider the wider legal effects of a smart contract (in relation the parties to it, as well as third parties), even if they are confident that it will not give rise to a legally binding contract. (This point is discussed in more detail in Part 6, below). [52]

III. WILL A SMART CONTRACT BE SUFFICIENT FOR THE PARTIES' NEEDS? WHAT MODELS COULD THEY USE TO MEET SUCH NEEDS?

Some commentators note that the scripting language of a smart contract may create less ambiguity than conventional contractual terms since it must be laid out in precise operational terms.[53] However, it is difficult to code all conceivable aspects of a legal relationship.[54]

- For instance, the logic of the programming language may not be able to define and incorporate all abstract legal concepts covered by "force majeure" or "good judgment." Moreover, when contracting electronically with consumers, information must be provided in clear terms, including the language or languages in which the agreement shall be available.[55] Consumers are not expected to understand software language.

[49] Article 1091 C.c. "Contracts are the law between the parties to an agreement" (lex privata). A contract is a voluntary assumption of liability in common law doctrine (in that, entering into a contract results in an assignment of rights between the parties to the contract).

[50] Article 1,278 C.c. "Contracts shall be binding, whatever the form under which they have been entered into, provided that they meet the essential conditions for their validity". *See also* Werbach & Cornell, *supra* note 4 at 36-39.

[51] The code's automated performance augments certainty but lacks flexibility compared to natural language. *See* Jeremy Sklaroff & Karen Levy, Smart Contracts and the Cost of Inflexibility, 166 U. Pa. L. Rev. 263, 286-291 (2017) (describing the evolution of EDI and its use in contracting and business processes).

[52] A distributed ledger is conceptually similar to any other system of IT-based messages used to create mutual assent. Any message that a node or a participant sends is a transaction or a contribution to the transaction by performing an action. *See* Douglas W. Arner, Ross P. Buckley, & Dirk A. Zetzsche, The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, 32, SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214 (hereinafter "Arner, Buckley & Zetzsche").

[53] Werbach & Cornell, *supra* note 4 at 38.

[54] *See* ISDA & Linklaters, Smart Contracts and Distributed Ledger – A Legal Perspective, 10-13 (August 2017), https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf .

[55] Art. 27 Electronic Commerce Law 34/2002 of 11 July. RCL 2002\1744, as last amended by Law No. 7/2010 of March 31, 2010, http://www.wipo.int/edocs/lexdocs/laws/es/es/es159es.pdf.

- The parties may need to utilize a broader contractual framework to define and document their wider relationship, or provide for governance arrangements. A smart contract may not be suited for this.
- Complex transactions governed by smart contracts would probably need a contractual framework that defines the non-operational clauses in natural language (*e.g.*, choice of law, competent jurisdiction or dispute resolution mechanisms).[56]
- As noted above, ensuring that variations and amendments to a smart contract will be legally binding is currently problematic from a legal perspective.[57]

For such reasons, both smart contracts and conventional natural language contracts may necessarily coexist in relation to the same (or related) subject matter. In such circumstances, courts may need to look at the entire legal framework within which a smart contract operates—that is, the smart contract, any related natural language contract, and any additional coding or documentation—in order to determine whether there is a legally binding contract between the parties and, if so, what its terms are.

Further there are different models of smart contracts.[58] The suitability of a specific model's ability to create a legally binding agreement will often depend on the different types of activities that a particular smart contract is intended to cover. The parties should consider whether the smart contract or a related natural language contract prevails, or how they work in combination. For instance, a banking consortium may decide to execute only its payments using smart contracts, with the rest of the contractual terms in natural language.

What follows is a consideration of some of the potential models for smart contracts.

DIFFERENT MODELS OF A SMART CONTRACT

EXTERNAL

- The code does not form the entirety of the parties' legal agreement, but merely automates the performance of some of its terms.

INTERNAL

- The code could encompass the entire agreement between the parties and supersedes other clauses written in natural language. Everything beyond the code merely explains the terms.
- Alternatively, the code could form only an integral part of the legally binding contract (rather than the entirety of the contract), and would supersede any other clauses written in natural language.

[56] There might be reasons not to automate everything. For example, an "event of default" gives a party the right but not the obligation, to terminate all outstanding transactions. But the decision tends to be subjective and the non-defaulting party may consider the nature of the default and other external factors. *See* ISDA & Linklaters *supra* note 44 at 10-13.

[57] SKLAROFF & LEVY, *supra* note 41 at 303.

[58] *See* ISDA & Linklaters *supra* note 44 at 14.

A. EXTERNAL MODEL – THE CONTRACT WRITTEN IN DIFFERENT LANGUAGES

The parties to a smart contract may decide to enter into a conventional agreement, known as an "external model." In such a case, the code does not form the entirety of the parties' legal agreement, but merely automates the performance of some of its terms. Therefore, the natural language version of the smart contract would prevail over the code and control the execution of the contract terms by the code.[59] The issues are similar to those raised by contracts written in different languages, where one version typically rules the others in the case of discrepancy.

When using the "external model," parties should make clear that the legal relationship is intended to be governed by the natural language version of the contract, rather than the code. Otherwise, courts could face difficult interpretational issues relating to the parties' intention. The outcome of such an assessment would be uncertain, given there is little legal guidance to courts at present, and the assessment would turn on the particular facts.

B. INTERNAL MODEL – THE CODE AS LAW

There are two potential types of "internal model" smart contracts:

- The code could encompass the entire agreement between the parties and supersedes other clauses written in natural language. Everything beyond the code merely explains the terms.[60] For instance, the DAO terms of service provided that the smart contract in the Ethereum blockchain controlled, with the natural language terms of use having no legal effect.[61]

- Alternatively, the code could form only an integral part of the legally binding contract (rather than the entirety of the contract), and would supersede any other clauses written in natural language. In such an "internal model" iteration, the smart contract may still utilize a natural language version for, say, non-operational clauses. But importantly, the code would be given legal effect. The novelty is that the code itself is an integral part of the agreement and not a translation of its terms. In operating certain clauses, the code forms the legally binding agreement between the parties.[62]

C. PROVIDING FOR FLEXIBILITY IN THE CHOSEN MODEL

Amending or varying a smart contract (or waiving a particular term) is currently problematic, at least in terms of the current state of the technology. Automatic and irrevocable performance could create

[59] *Id.* at 16-17.

[60] Werbach & Cornell, *supra* note 4 at 16. *See also Id.* at 20-30 ("if a court concludes it (the conventional contract) better reflects the parties' meeting of the minds, it would be trying to supersede the smart contract, not interpret it.").

[61] Christoph Jentzsch, Decentralized Autonomous Organization to Automate Governance Final Draft – Under Review, https://download.slock.it/public/DAO/WhitePaper.pdf. On or about April 29, 2016, Slock.it deployed The DAO code on the Ethereum Blockchain, as a set of pre-programmed instructions. This code was to govern how The DAO was to operate. The DAO tried to supersede all legal enforcement with smart contracts. The DAO white paper stated that it was solely for "educational purposes." The DAO terms of service specifically provided that the smart contract in the Ethereum blockchain was the controlling legal authority. Any human-readable documents or explanations, including those on the website, "were merely offered for educational purposes and do not supersede or modify the express terms of The DAO's code set forth on the blockchain," The DAO, https://daohub.org/explainer.html. (no longer available as of June 3, 2018). An "attack" diverted 3.6 million of ether (ETH) from The DAO to another blockchain address controlled by the attackers. Interestingly, the misappropriation of funds did not require a change or "hack" to the code. The diversion of funds by the "attackers" was permitted due to a flaw in the original code. However, this was not the parties' intention in developing the project, and the consensus by the majority ended using a "hard fork."

[62] Werbach & Cornell, *supra* note 4 at 36-37.

difficulties in cases of coding mistakes or judicial enforcement, or in situations where a party is simply amenable to extending the time for performance or modifying obligations.

Similarly, when an electronic contract is contrary to law or the interest of consumers, a party can, in many jurisdictions, petition a court to stop the contract's automatic performance. (This is the case, for example, under Spanish law.)[63] When a change in circumstances (*e.g.*, export bans or trade sanctions) makes performance illegal, the parties may need to suspend performance. Often the law requires the ability to rectify errors in a way that may be difficult to implement on an immutable distributed ledger.

Amendments or modifications are relatively easy in conventional contracts, and parties can waive provisions if they so choose. However, smart contracts lack semantic and enforcement flexibility compared to conventional contracts.[64] Computer code can only tolerate precise conditional instructions ("if-then"). For instance, there is no flexibility for the parties to incorporate a term that has one meaning at the time of execution and can be interpreted differently during the performance phase.

Concepts such as "good faith," "commercially reasonable," or "force majeure" in contracts often provide the parties with the necessary flexibility to agree on a particular interpretation of the contractual terms or even renegotiate them to avoid litigation. Incorporation of such provisions in the context of smart legal contracts would be difficult, if not impossible.

Such considerations should be factored into the selection of smart contract model and the governance framework within which it operates, which could include ameliorating provisions to address the fact that performance is inevitable once a smart contract is initiated.

Some smart contracts are easier to modify than others, leading to the distinction by some commentators between "soft" and "hard" smart contracts.[65] However, the inflexibility of an automated performance mechanism within a smart contract makes it potentially impossible to alter a smart contract during its performance phase, unless the code has in some way provided for the possibility of modification (perhaps in predictive programming).

Multi-signature arrangements or requirements could be explored as a mechanism to lock, unlock, or amend smart contracts.[66] For instance, a smart contract intended to have legally binding effect could include a provision that checks for superseding smart contracts countersigned by the parties to the original contracts.

[63] *See* Art. 30 of the (E-Commerce) Law No. 34/ 2002 of July 11, 2002 (as amended by Law No. 7/2010 of March 31, 2010), http://www.wipo.int/wipolex/en/details.jsp?id=11832. *See* Art. 15 of Law 22/2007, Of July 11, On Distance Marketing Of Financial Services To Consumers, https://www.global-regulation.com/translation/spain/1445417/law-22-2007%252c-of-july-11%252c-on-distance-marketing-of-financial-services-to-consumers.html. "Article 15. 1) can exercise the action of ceasefire against the conduct contrary to this Act that injured both collective and diffuse interests of consumers and users. 2) the cessation activities are directed to obtain a ruling which condemn the respondent to cease the conduct contrary to this Act and to prohibit their future repetition. Likewise, the action may exercise to prohibit conducting a behavior when this is complete at the time of bringing the action, if there are sufficient indications that make fear your reiteration of immediate mode. (...)"

[64] SKLAROFF & LEVY, *supra* note 41, at 23.

[65] *See* Raskin, *supra* note 24 at 309-311.

[66] J. Dax Hansen and Joshua Boehm, Treatment of Bitcoin Under U.S. Property Law, 15, (Mar. 2017), https://www.virtualcurrencyreport.com/wp-content/uploads/sites/13/2017/03/2016_ALL_Property-Law-Bitcoin_onesheet.pdf.

Without the development of mechanisms that allow contracting parties to address changed circumstances and more easily adjust terms, the utility of stand-alone smart contracts intended to have legal effect may be limited, particularly in complex transactions. In these circumstances, the necessary flexibility and management of contract amendments may be provided by augmenting smart contracts with a master agreement or a conventional (natural language) contract, or an over arching participation or governance framework having legally binding effect.

IV. WHAT IS THE GOVERNING LAW OF A SMART CONTRACT?

Blockchain technology exists on a network of computers with nodes and users typically based all over the world.[67] Which jurisdiction's laws will apply to a smart contract on such a distributed network?

As a general matter, the parties to an agreement can contractually select the law applicable to a smart contract. However, in some jurisdictions (*e.g.*, Spain), the governing law selected by the parties must have some connection with the business in question. If a smart legal contract is litigated before a Spanish court, but does not include a choice-of-law provision, the Spanish Civil Code's Preliminary Title provides legal criteria for the court to determine the governing law of the contract.[68] Most developed legal systems have similar legislation determining the issue, often implemented pursuant to international treaties, and often augmented by a body of conflict-of-laws rulings to determine the issue when the parties have not provided for it.

In the United States, choice of law issues are typically a matter of individual state policy and jurisprudence. As a general matter,[69] when the parties to an agreement have expressly selected the law of a particular state, or if the court concludes from the provisions of an agreement that the parties wished to have the law of a particular state applied, the court will apply the rights and duties of such state.[70] However, a U.S. court will not apply the rights and duties of a state if: 1) the chosen state does not have a "substantial" relationship with either party, and there is no reasonable basis for the parties' choice; or 2) applying the chosen state's law would be "contrary to a fundamental policy of a state which has a materially greater interest than the chosen state."[71] In the absence of an express selection of a state of applicable law, the Restatement (Second) of Conflicts of Law looks to the state that has "the most significant relationship to the transaction and the parties," as evidenced by the place of contracting, the place of negotiation, the place of performance, the location of the subject matter of the contract, and the domicile, residence, nationality, place of incorporation, or place of business of the parties.[72]

[67] Wulf A. Kaal and Graig Calcaterra, Crypto Transaction Dispute Resolution, 31, SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992962##. For instance, the Ethereum white paper answers the question where the code is executed, in terms of physical hardware as follows: "This has a simple answer: the process of executing contract code is part of the definition of the state transition function, which is part of the block validation algorithm, so if a transaction is added into block B the code execution spawned by that transaction will be executed by all nodes, now and in the future, that download and validate block B. *See* Buterin, *supra* note 4.

[68] Art. 1262 C.c. and 10.5 Preliminary Title of the Spain's Civil Code, http://www.boe.es/buscar/pdf/1889/BOE-A-1889-4763-consolidado.pdf.

[69] While the Restatement (Second) of Conflicts of Law (Am. Law Inst. 1971) is widely followed in many states, other choice of law rules may be applied, for example: 1) lex loci contractus ("the place of contract") has been applied in Alabama, Georgia, and Maryland; 2) the "governmental interest" test has been applied in California; 3) the doctronie of renvoi has been applied in Maryland; and 4) legal commentator Robert Lefar's "Five Choice-Influencing Factors" have been applied in North Dakota.

[70] Restatement (Second) of Conflicts of Law § 187 (Am. Law Inst. 1971).

[71] *Id.* at Comments.

[72] *Id.* at § 188.

AS A GENERAL MATTER, THE PARTIES TO AN AGREEMENT CAN CONTRACTUALLY SELECT THE LAW APPLICABLE TO A SMART CONTRACT. IN THE UNITED STATES, CHOICE OF LAW ISSUES ARE TYPICALLY A MATTER OF INDIVIDUAL STATE POLICY AND JURISPRUDENCE.

Parties should keep in mind that U.S. courts may consider the relationships of the parties and the manner in which the contract was presented when determining the applicable state law.[73] Courts may be wary of contracts that are "drafted unilaterally by the dominant party and then presented on a 'take-it-or-leave-it' basis to the weaker party who has no real opportunity to bargain about its terms."[74] For contracts on a blockchain (as discussed in Part 1 of this white paper), the structure of the offer, acceptance, and consideration may inform U.S. courts as to whether there was a "dominant party" who made a "take-it-or-leave-it" offer when determining the applicable state law.

In Europe, where the parties to a smart legal contract are located in different countries, but have not chosen a specific choice of law, the E.U. Regulation "Rome I" can help a court determine the applicable law for that smart contract. The following general principles are set forth in Rome I:

- "A contract for the provision of services shall be governed by the law of the country where the service provider has his permanent residence."[75]
- In case of financial instruments negotiated in a multilateral trading facility, "a contract concluded within a multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments, in accordance with non-discretionary rules and governed by a single law, shall be governed by that law."[76]
- Such principles could be applicable by analogy to other areas.[77] For instance, rights *in rem* (title registration or real estate) are typically linked to the law of the country where the property is registered or located.[78]
- The law of the country where the party of "the most characteristic performance" has its permanent residence will apply in residual cases where the smart contract is not covered by any of the other criteria, or where more than one could be applied.

[73] *Id.* at § 187.

[74] *Id.*

[75] "Rome I", which is directly applicable in Spain, rules the applicable law to international contractual obligations. *See* Article 4.1. (b) Regulation E.U. 593/2008, "Rome I", http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0593.

[76] *Id.*; Art. 4. 1. (h). Regulation E.U. 593/2008 "Financial Instrument" as defined by Article 4(1), point (17) of Directive 2004/39/EC (MiFID) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004L0039.

[77] Article 4.1. (h) Regulation E.U. 593/2008, "Roma I", http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0593. Another example would be CREST for dematerialized securities, which operates under the authority or the Uncertificated Securities Regulations 2001. *See* Ernst and Young, Hogan Lovells, & Innovate Finance, Blockchain, DLT and the Capital Markets Journey: Navigating the Regulatory and Legal Landscape, 23 (October 2016), https://www.hoganlovells.com/-/media/hogan-lovells/pdf/publication/2016/hogan_lovells_innovate_finance_and_ey_blockchain-digital_spread.pdf?la=en.

[78] Article 4.1.(c) of the Regulation E.U. 593/2008.

- Contracts executed electronically with consumers are performed where the consumer has his permanent address.[79]
- Where it cannot be determined otherwise, the law of the country that is more closely connected to the smart contract shall also apply.[80]

As noted above, most other developed legal systems have legislation speaking to choice-of-law issues, often implemented pursuant to international treaties and typically augmented by court decisions within a body of "conflict of laws" principles.

Although such laws exist to help determine the issue, the parties to a smart legal contract may wish to avoid the uncertainties of not having specifically provided for the law that is to govern and construe their legal agreement. The choice of law governing a smart legal contract should take into account the blockchain design, its business case, technical complexity, number of participants and jurisdictional reach, among other considerations. [81]

V. JUDICIAL ENFORCEMENT OF SMART LEGAL CONTRACTS

When a smart contract constitutes a smart legal contract (*i.e.*, a legally binding contract), a party to that contract will face certain challenges in seeking judicial enforcement. Some may argue that it is impossible to breach a smart contract because the code is immutable and self-executing. However, that view fails to take into account that people, with varying understandings and interpretations, are (ultimately) the parties to smart contracts. Disputes will inevitably arise as to issues surrounding the parties' intent.

Additional disputes may arise due to coding errors or issues relating to the functionality of the smart contract platform itself. Indeed, the very nature of blockchain is likely to present courts with novel issues, or at the very least with novel applications of established judicial principles.

A. LIMITS TO ENFORCEMENT BY THE COURTS

The nature of blockchain, distributed ledger, smart legal contracts, and the parties thereto will inject complex issues into judicial proceedings. Such issues will likely include:

- Whether the court has personal jurisdiction over the parties to the contract (assuming those parties can be identified) or, alternatively, whether the court has jurisdiction over the assets at issue.
- Whether the court has personal jurisdiction over the smart contract platform itself.
- Whether the court has subject matter jurisdiction over the dispute, including consideration of whether and to what extent judicial enforcement is compatible with the "immutability" of distributed ledgers and public policy.

[79] Art. 29 Electronic Commerce Law 34/2002 of 11 July. RCL 2002\1744, as last amended by Law No. 7/2010 of March 31, 2010, http://www.wipo.int/edocs/lexdocs/laws/es/es/es159es.pdf.

[80] *Id.*; Art. 4. Paragraph 2, 3 and 4. Similarly, article 4 of the former E.U. Rome Convention of 1980 provided that, in absence of a specific choice by the parties, the applicable law will be that of the location where "the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporated, its central administration." *See* Rome Convention of 1980 on the law applicable to contractual obligations, http://eur-lex.europa.eu/legal content/EN/ALL/?uri=CELEX:41998A0126.

[81] Arner, Buckley & Zetzsche, *supra* note 42 at 23.

- In the case of a hybrid contract (*i.e.*, a contract in which parts of the contract exist in traditional written form and parts of the contract exist in a self-executing smart contract), does the written contract or the code control?
- What law is applicable to the parties' dispute, an issue traditionally tied to factors such as the place of contracting, location of the parties, location of performance, location of the subject matter of the contract, and the public policies of the forum.
- How would a court decision to reverse a transaction effected by a smart contract be achieved where, for example, the court has determined that a smart contract is void (*i.e.*, never existed) or voidable (*i.e.*, the aggrieved party can cancel the contract), because of, for instance, a mistake, lack of capacity, or duress? Enforcement of a remedy to reverse a transaction in a distributed ledger may be difficult, if not impossible, due to numerous factors, including the speed with which digital assets can be transferred out of the smart contract platform and principles relating to good faith transfers in due course.
- A plaintiff's remedy may be limited to monetary compensation/damages.[82] But how would a court enforce a monetary damage award against far flung, potentially anonymous entities?
- Because a smart contract performs automatically once initiated, how would a court enforce a remedy that excuses future performance?
- If available, how would other remedies—such as specific performance for a breach of contract—work in relation to a smart contract?
- If the alleged wrongdoing was on the part of the platform itself, courts and litigants would have to grapple with additional issues, such as where the ledger is located and who needs to be served.[83]

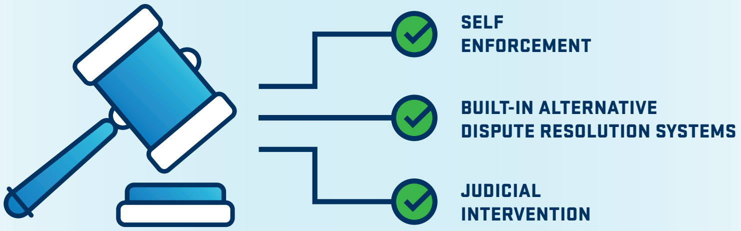
B. GOVERNANCE AND AUTOMATIC ENFORCEMENT MECHANISMS

Unless and until there is sufficient confidence in the enforceability of a smart legal contract, parties intending for their transaction to have legally binding effect may wish to consider incorporating arbitral clauses, governance and/or automatic enforcement mechanisms to limit the circumstances in which they will require judicial intervention or to facilitate enforcement of arbitral or judicial decisions.

For instance, parties, or the platform itself, may wish to build in an escrow procedure (despite the fact that such a procedure may be perceived as undermining some of the advantages of a smart contract). The parties also may consider building into their smart contract mechanisms to stop automatic performance in the case of a dispute or, alternatively, mechanisms to permit the claw back of funds or other assets by giving the smart contract access to certain accounts funded by the parties. Such self-enforcement mechanisms occur in current commercial arrangements. For instance, banks include in their account agreements a statement regarding the bank's ability to credit or debit an account in the event of an error.[84]

[82] *See*, *e.g.*, Spanish Civil Code, Art. 1307 C.c.
[83] *See* Arner, Buckley & Zetzsche, *supra* note 42 at 32.
[84] Additional examples of self-enforcement mechanisms exist in various areas of U.S. law. *See* U.C.C. § 9-609 (a secured creditor, after

SMART CONTRACTS GOVERNANCE AND ENFORCEMENT



SELF ENFORCEMENT

BUILT-IN ALTERNATIVE DISPUTE RESOLUTION SYSTEMS

JUDICIAL INTERVENTION

Contracting parties also may consider utilizing a platform that has alternative dispute resolution mechanisms built into it; these types of mechanisms have been referred to as alternative dispute resolution mechanisms.[85] Such mechanisms may be most appropriate for smart contracts in decentralized ledgers. However, as with other alternative dispute resolution procedures, such as arbitration, there likely will remain the need for some degree of judicial review and/or enforcement.

In some instances, enforcement of a platform's internal dispute resolution mechanism may require judicial intervention, compelling participation by another party to the transaction or compliance with the decision rendered in accordance with the agreed-to dispute resolution procedure.[86]

Many market participants have expressed the hope that smart contracts will eliminate, or at least reduce, the need for contract litigation. At this point, however, it appears that smart contract self-enforcement mechanisms will not be able to supplant completely the need for judicial review and enforcement procedures.[87]

VI. UNDERSTANDING THE POTENTIAL SCOPE OF LIABILITY IN RELATION TO SMART CONTRACTS

Liability in relation to smart contracts may, of course, include contractual liability for breach. Principles of contractual liability are well established and understood in most developed legal systems. These well-established principles will, however, require adaption when applied to smart contracts (Parts 1 and 2 of this chapter demonstrate how contractual principles more generally might apply in relation to the question of formation of a smart legal contract).

default, has the right to "take possession of the collateral" and/or "render the equipment unusable" without judicial process so long as the action "proceeds without breach of the peace"); *see also* Raskin, *supra* note 24 at 304, 330-33 (discussing examples of self-help mechanisms under U.S. law). Self-enforcement mechanisms also exist in jurisdictions other than the United States. *See, e.g.*, Spanish Civil Code Art. 592 C.c. (setting out landowner's right to cut roots and branches of a tree planted on neighboring land when they invade the landowner's private property).

[85] Several modalities of alternative dispute resolution mechanisms internal to the smart contract platform exist, including solutions from existing Aragon or Ricardian Contracts (consisting of a pool of private judges or arbitrators, who act semi-anonymously) to more anonymous proposals for dispute resolution modalities based on distributed jurisdictional mechanisms. Distributed jurisdictional mechanisms could include an "open source platform ecosystem of smart contracting dispute resolution that allows users to opt into the conflict resolution mechanisms." *See* KAAL & CALCATERRA, *supra* note 57, at 44-57.

[86] *See, e.g.*, Federal Arbitration Act, 9 U.S.C. § 1 *et seq.* (statutorily setting out procedures for enforcement of arbitration clauses and for review and enforcement of arbitration decisions).

[87] Werbach & Cornell, *supra* note 4 at 313, 353. Indeed, the self-help mechanisms currently found in the law traditionally are judicially supervised. For instance, when creditors disturb the peace in the United States, a judge may restrain their self-help rights. *Id.* at 347. The role of courts cannot entirely be replaced by self-enforcement mechanisms in Spain either, since the right of a judicial review by the parties to any legal agreement is protected by Art. 24 of Spain's 1978 Constitution, https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf.

While contractual breach is not generally the focus of this Part (Chapter 2 deals with some aspects of contractual breach in relation to smart contracts), a general observation relating to non-contractual liability arising out of contractual breach can be made at this point. In many jurisdictions, a party is liable for damages whenever he or she has acted negligently in performing contractual obligations (*e.g.*, in Spain).[88] A party acts negligently when he or she breaches a "reasonable duty of care."[89] How does the lack of a "reasonable duty of care" translate to smart contracts? It could refer to routine technical infractions in operating a blockchain (*e.g.*, security breaches caused by failure to update software, or deficient storage by the users of the private keys related to a digital asset). However, a breach of the "duty of care" would be extremely difficult to prove if related to any contractual failures of predictive performance by algorithms.[90]

Regardless of whether a smart contract has legally binding effect, other kinds of (non-contractual) liabilities might arise in connection with the transaction, both between the parties and vis-à-vis third parties. The smart contract transaction, even if it does not constitute a legally binding contract, still may effect (or change) in some way the legal relations between the parties (for example, by transferring ownership of an asset). This Part considers the potential scope of effects and resulting liabilities.

Many potential non-contractual liabilities may arise in relation to particular transactions accomplished through blockchains or automated contracts. For example, claims for fraud, unfair and deceptive trade practices, or theft may exist outside of the contract. Further, additional liabilities may arise relating to the technology platform itself, as a whole, rather than in relation to the individual smart contracts on the platform. Such issues might include ledger transparency and data privacy, insider trading and market abuse, identity theft, cybersecurity risks, and various operational risks (all of which are beyond the scope of this chapter).[91]

Both common law systems (such as the United States) and civil law systems (such as Spain) typically include liability in tort for negligence, fraud, and breaches of fiduciary duty. Laws aimed at preventing unfair and deceptive trade practices may also apply.[92] Further, in the context of product liability, legal systems may also impose strict liability (without the need for establishing certain traditional tort principles). Will these kinds of tortious liabilities potentially arise in relation to smart contracts?

However, as some commentators have noted in relation to software or automated contracts, current liability regimes governing intentional misconduct, negligence, and strict liability align poorly with algorithms.[93] In the U.S. context, for example, it has been said that "[t]he law of software liability seems to be strangely undeveloped, considering the size of the software industry and the infiltration of software into virtually every aspect our lives… And though legal commentators have been predicting a great expansion of liability for defective software since the 1980's…it has not occurred."[94]

[88] Art. 1101 C.c.

[89] Articles 1719 C.c. and 1094 C.c.

[90] A leading article notes that it is nearly impossible to prove that a software program was written negligently. Arner, Buckley, Zetzsche, *supra* note 42 at 13-20.

[91] "The fact that nodes sign up to the network (*i.e.,* buy /sell / mine Bitcoins) without AML/CTF checks may evidence ignorance of the law but not the law's inapplicability". Arner, Buckley, Zetzsche, *supra* note 42 at 33.

[92] *See*, *e.g.*, N.Y. General Business Law §§ 349 *et seq.*; Fla. Stat. §§ 501.201 *et seq.*

[93] Yesha Yadav, The Failure of Liability in Modern Markets, 102 Va. L. Rev. 1031, 1073-1100 (2016).

[94] David Polin, Proof of Manufacturer's Liability for Defective Software, 68 Am. Jur. Proof of Facts (3d, 2018).

It remains to be seen whether and how these kinds of tortious liabilities will arise in relation to smart contracts, whether between the parties or in relation to a third party. However, a few general observations can be made at this point.

”Broadly speaking[,] a tort is a civil wrong, other than a breach of contract, for which the court provide[s] a remedy in the form of an action for damages.”[95] In the United States, tort law is determined at the state level and may vary from state to state.[96] It is, however, an oft-recited principle that, in general, a party may not recover both in contract and in tort for a frustration of its contractual economic expectations.[97] Where this principle is in fact applicable, it may function to narrow the scope of recovery in the case of, say, an incorrectly (and negligently) coded smart contract, which, depending on the facts, may cause no physical harm to persons or property, but a substantial economic damage.[98]

An alternative standard of tortious liability - strict liability - may be applied in certain jurisdictions even in the absence of fault. In the context of strict product liability, for example, a plaintiff need generally only prove the existence of the defect, the damage, and a causal relationship between the defect and damage.[99] The rule against recovery of pure economic loss, referred to above, may also limit recovery of damages for strict liability in tort under U.S. law.[100]

A similar position applies under the Spanish Product Liability Act, implementing the European Directive on Product Liability (1985), which applies strict liability to manufactures, importers of products, and other intermediaries in the supply chain.[101] Strict liability is intended to protect consumers in cases of defective products that caused injury, death, or damage to personal property, but excludes economic loss.[102] It is unclear whether and how strict liability principles would apply to smart contracts.[103]

VII. CONCLUSION

[95] William Lloyd Prosser & W. Page Keeton, Prosser and Keeton on the Law of Torts (West 5th ed., 1984) at 692-93.

[96] Most states use the ALI’s Restatement of Torts as the basis for their tort laws. Restatement of the Law (Second) Torts (Am. Law Inst. 1965); Restatement of the Law (Third) Torts: Products Liability (Am. Law Inst. 2000).

[97] *See* Feldman v. Kohler Co. 918 S.W. 2d 615 (Tex. App. 1996) writ denied (“In the context of defective computer software, this is an issue of first impression for this Court. Nonetheless, the existence of a duty is a question of law for a court to decide from the facts surrounding the occurrence in question”). *See also* Mitchell v. Missouri-Kansas-Texas R.R., 786 S.W.2d 659, 662 (Tex. 1990).

[98] Hou-Tex, Inc. v. Landmark Graphics, 26 S.W.3d 103 (Tex. App. 2000). The court applied the “economic loss” doctrine to limit the recovery for damages that are not associated with personal injuries or property damages. The court dealt with the issue of the liability of a software provider (Landmark Graphics) to a third party (Hou-Tex) that had received services from a contractor using the software. Hou-Tex (an oil and gas company) drilled a hole after its independent contractor helped choose the drilling site by using a software licensed by Landmark Graphics. The software contained a “bug” that miscalculated data from plots of land with irregular boundaries. As a consequence, the site where the hole was drilled was incorrect. Landmark knew about the “bug” in advance and had corrected the problem in an updated version of the software sent to some clients, but not to Hou-Tex’s contractor, who wrongly advised the site for the drilling. Hou-Tex suffered economic damages (but no physical harm to persons or its property) for the costs in drilling a dry well. Applying the “economic loss” doctrine, the court concluded that Hou-Tex had no right to recover lost profits and followed the Fifth Circuit Court of Appeals in analyzing Texas law. *See also* Hininger v. Case Corp., 23 F.3d 124, 125 (5th Cir. 1994) (where product purchaser sued remote component part manufacturer for product defect and economic loss).

[99] *See*, *e.g.*, HDM Flugservice GmbH v. Parker Hannifin Corp., 332 F.3d 1025, 1030 (6th Cir. 2003).

[100] Under U.S. law, strict liability in tort is imposed on the theory that “the costs of damaging events due to defectively dangerous products can best be borne by the enterprises who make and sell these products.” It is generally applied to limited categories of products such as drugs, food and beverages, and motor vehicles. Prosser & Keeton, *supra* note 85 at 692-93.

[101] Spain’s Product Liability Act (Ley 22/94 de responsabilidad civil por daños causados por productos defectuosos, hereinafter the Act), B.O.E. (7 July 1994) Amended by Ley 14/2000 of 19 December.

[102] *See also* K. Alheit, “The Applicability of the E.U. Product Liability Directive to software” at 200, https://www.jstor.org/stable/23251124?seq=1#page_scan_tab_contents.

[103] The E.U. Product Liability Directive (1985) is under consultation by the European Commission: “The [E.U.] Commission has launched an expert group on liability to explore the effect of these developments in detail. (…) The expert group will assess whether the overall liability regime is adequate to facilitate the uptake of new technologies by fostering investment stability and consumer trust.” *See* EU Report on May 2018 on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), 8-10, https://ec.europa.eu/docsroom/documents/29233.

A blockchain or distributed ledger is similar to any other IT-based message platform used to agree on transactions. Courts have already accepted that email messages can give rise to legally binding contracts in many jurisdictions. Automated performance is common in equities markets and algorithm trading. Existing contract laws (including e-commerce laws), therefore, may in many instances suffice in the case of the formation of smart legal contracts.

The analysis in Part 1 supports the conclusion that, in certain jurisdictions, such as the United States and Spain, in certain circumstances smart contracts may be considered legally binding contracts. A smart contract may contain some legally binding clauses, if the parties so agree. However, the analysis in Part 1 also illustrates that it would be wrong to assume that conclusions reached for one jurisdiction will necessarily be true of another. (Contract requirements differ between common law and civil law, for example.) Because blockchains do not recognize borders, it will be necessary to consider where any proposed smart contract deployment intends to operate internationally.

It is worth noting that existing smart contract use cases do not replace (the entirety of) natural language contracts with computer code, particularly in the case of high-stakes or complex transactions. This is the case for a range of reasons, including the lack of flexibility of the scripting language. Parties entering into legally binding contracts using smart contracts should carefully consider control mechanisms and governance that may impact their ability to modify the original contract. If greater flexibility is needed, additional control measures may be required. Ultimately, technology developments may provide the needed solutions.

The parties should specify the choice of law and dispute settlement mechanisms governing the smart legal contract, taking into account the blockchain design, its business case, technical complexity, number of participants, and jurisdictional reach, among other considerations.

For those developing and deploying smart contracts, it will be important to bear in mind that liability (whether or not the smart contract has legally binding contractual effect) could extend beyond the parties themselves. Entities engaging in activities relating to smart contracts must factor such risks in their governance, particularly when dealing with consumers and investment stability.

CHAPTER 2: SMART CONTRACTS, BLOCKCHAIN, AND COMMERCIAL LAW

Margo Tank, David Whitaker, and Patricia Fry[104]

Although the concepts are not new,[105] blockchain technology and smart contracts have generated a lot of interest in the past several years. Both constructs have been acclaimed as employing technological means to avoid intermediaries and significantly reduce transaction times and costs. Legislation has been enacted in a few states and introduced in others declaring that (i) smart contracts are enforceable and (ii) records and signatures created, secured, or retained using a blockchain platform constitute electronic records and signatures under applicable law.[106] Other proposed legislation calls for studying the potential use of blockchain or smart contracts in certain types of transactions.[107] This chapter demonstrates that existing law, in the form of the federal Electronic Signatures in Global and National Commerce Act ("ESIGN")[108] and the Uniform Electronic Transactions Act ("UETA")[109] already recognizes, enables, and validates the use and enforceability of both (i) smart contracts and (ii) electronic records and signatures created, secured, or retained by utilizing a blockchain platform.[110]

This chapter first provides background by describing smart contracts and blockchain technology and illustrating their use in hypothetical commercial transactions. We then analyze the operation of existing commercial law in such cases, with particular focus on the UETA and federal ESIGN. Examining the text and commentary associated with those bodies of law, we discuss how each applies to support and enforce the expectations of those using smart contracts and blockchain processes.

[104] Margo Tank and David Whitaker are Partners at DLA Piper LLP (U.S.) and advise commercial enterprises and technology companies on the full spectrum of regulatory compliance matters related to the use of electronic signatures and records to enable digital transactions offered online, via mobile devices, smart contracts, and blockchain. Ms. Tank played a lead role advocating enactment of the ESIGN Act, and Mr. Whitaker participated in the drafting of the UETA and chaired the Task Force on Scope. They both serve as Co-Reporters for SPeRS and are counsel to the Electronic Signature & Records Association. Patricia Fry is the Edward W. Hinton Professor of Law Emeritus, University of Missouri-Columbia School of Law, and a Life Member of the Uniform Law Commission. She chaired the drafting committee that produced the UETA. The authors would also like to thank Andrew Grant, an associate at DLA Piper, for his assistance with this chapter.

[105] The use of cryptology to secure a chain of blocks of data was first described in 1991; *see* Stuart Haber & W. Scott Stornetta, How to Time-Stamp A Digital Document, 3 J. Cryptology 99, 99-111. The term "smart contracts" was coined in 1994 when cryptographer Nick Szabo first published an article titled "Smart Contracts", available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[106] *See*, *e.g.*, Ariz. Rev. Stat. 44-7061 (2017); Nev. S.B. 398 (2017); Tenn. Rev. Stat. (2018); Cal. A.B. 2658 (2018); Ill. H.B. 2257 (2018); NY S.B. 8858 (2018); NY A.B. A8780 (2017); and Ohio S.B. 300 (2018) .

[107] *See, e.g.*, Del. S. 69 (2017) (authorizing use of blockchain for corporate records); Ill. H.J.R. 25 (2017) (establishing a blockchain task force); Colo. S.86 (2018) (directing chief information officer to evaluate using blockchain in government systems); *see also* Pete Rizzo, Delaware Governor Signs Blockchain Bill Into Law, Coindesk (July 24, 2017, 1:30 PM), https://www.coindesk.com/delaware-governor-signs-blockchain-legislationlaw/.

[108] 15 U.S.C. § 7001, *et seq.* (2000).

[109] Approved and recommended for enactment by the states by the Uniform Law Conference in 1999 and enacted in 47 states, the U.S. Virgin Islands and the District of Columbia.

[110] *See* text accompanying fn. 152, *et seq.*

I. BACKGROUND

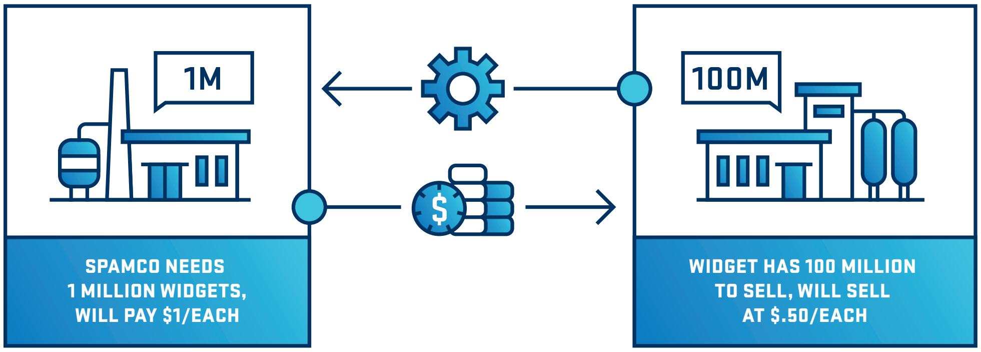
A smart contract is computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions. The code can be stored and processed on a distributed ledger and would write any resulting change into the distributed ledger. A smart contract may, but need not, involve the employment of a blockchain. When using a smart contract incorporating blockchain technology, the underlying algorithm utilizes a consensus mechanism. The original illustration of a smart contract, given by Nick Szabo, was simply a vending machine that dispenses goods upon payment of a specified sum.[111]

THE ORIGINAL ILLUSTRATION OF A SMART CONTRACT, GIVEN BY NICK SZABO, WAS SIMPLY A VENDING MACHINE THAT DISPENSED GOODS UPON PAYMENT OF A SPECIFIED SUM.

As a more complex illustration of a smart contract that does not employ a blockchain, consider the following hypothetical transaction between Spamco, LLC ("Spamco") and Widget, Inc. ("Widget"). Spamco uses an electronic agent to determine when to purchase widgets—based on need combined with available prices—and how many widgets to purchase. Widget sells widgets and uses an electronic agent to negotiate its contracts based on its available supply and the market in general. Spamco needs 1 million widgets and is willing to pay up to $1 each; Widget has 100 million widgets it can sell and is willing to sell them at $0.50 apiece. Spamco and Widget enter into negotiations using electronic agents that have been programmed to establish delivery terms, volumes, and price based upon established parameters. In this manner, Spamco and Widget reach an agreement through the interaction of the electronic agents; Spamco receives the needed widgets and pays Widget the agreed-upon amount. At no point during the transaction, after the electronic agents were programmed and deployed, did any human participate in or review the negotiation or resulting agreement, nor was a blockchain necessary to execute or perform the transaction.

[111] Szabo, *supra* note 105.

TRANSACTION BETWEEN SPAMCO, LLC & WIDGET, INC


1M
100M
$
SPAMCO NEEDS 1 MILLION WIDGETS, WILL PAY $1/EACH
WIDGET HAS 100 MILLION TO SELL, WILL SELL AT $.50/EACH

No human review or negotiation in agreement.

That being said, there is a significant potential synergy between smart contracts and blockchain. The term “blockchain” has been defined in various ways, not all of which are fully compatible, but generally comprise groups of entries of records of multiple transactions collected into a “block.”[112] Each block of entries, recorded in electronic form, otherwise called an electronic record, contains a cryptographic hash of the preceding block, linking the block to the rest of the blockchain. The chain of blocks containing electronic records is stored as a “ledger,” also an electronic record, which can be distributed or not, *i.e.*, disseminated through numerous computers, usually without a central repository. Once the electronic record is entered, it is immutable or at least if altered, the alteration can be detected, both through the cryptography used and from the disseminated nature of the ledger.[113]

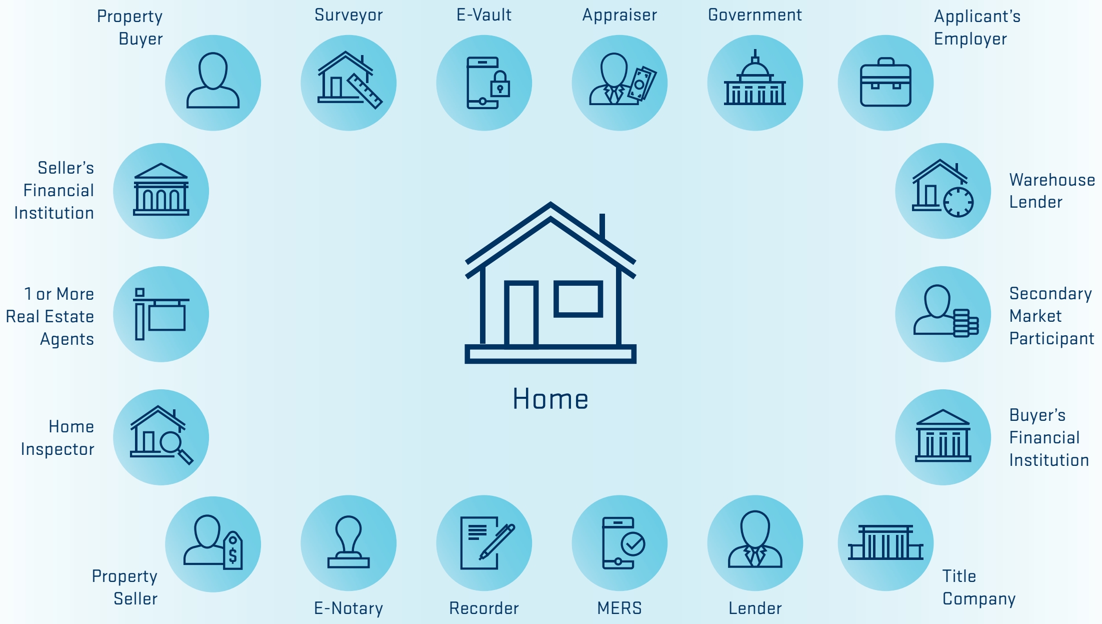
To illustrate the potential synergies between a smart contract and a blockchain, consider the process of issuing the final approval and loan commitment for a residential mortgage loan. Those routinely participating in the process include the applicant, the applicant’s financial institution and employer, the lender, one or more real estate agents, the seller of the property, a home inspector, a surveyor, an appraiser, a title company, and potentially even the government (through submission of a Form 4506-T to the IRS for tax information concerning the applicant). The final approval to lend requires delivery of trusted data from a variety of sources to the lender, evaluation of that data, and issuance of the final commitment.[114]

[112] For our purposes, the term “blockchain” is defined in our Lexicon, above, as “a specific type of distributed ledger technology that organizes data into blocks that are “chained” together chronologically by a cryptographic hash function and confirmed by a consensus mechanism.” For further discussion of what constitutes blockchain technology, *see generally* NIST Dylan Yaga *et al.*, Draft NISTIR 8202:, Blockchain Technology Overview, NIST (Jan. 24, 2018), https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf (hereinafter “NIST Draft”); *see also* ASC X9 Study Group Report, Distributed Ledger and Blockchain Technology Study Group (Apr. 6, 2018), https://x9.org/wp-content/uploads/2018/04/Distributed-Ledger-and-Blockchain-Technology-Study-Group-Report-FINAL.pdf.

[113] For further definitions *see generally*, Lexicon *supra*; Ameer Rosic, Smart Contracts: The Blockchain Technology That Will Replace Lawyers, Blockgeeks, https://blockgeeks.com/guides/smart-contracts, (last visited Feb. 4, 2018); Uniform Regulation of Virtual-Currency Businesses Act, Prefatory Note, 4, http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/URVCBA_Final_2017oct9.pdf; Kate Addicott, Up Close with Blockchain Technology, IBM (Jan. 22, 2018), https://www.ibm.com/blogs/events/think-2018-presents/think-2018-blockchain.

[114] For another example of a blockchain-based system for tracking information and the progress of a transaction, *see* Up Close with Blockchain Technology, (describing a process used for the international shipment of flowers).

HOME PURCHASE TRANSACTION: POTENTIAL OF SMART CONTRACTS & BLOCKCHAIN



One trusted environment.
All points of communication are tracked and updated in a single, reliable location.
No point of data may be changed, and the source of that data may be determined with certainty.

With the use of blockchain technology, all of that information may be brought together into one trusted environment that can be accessed by the lender. Inspections, appraisals, approvals, and all points of communication are tracked and updated in a single, reliable location. All of the documentation and each signature may be accessed, no point of data may be changed, and the source of that data may be determined with certainty. When all the information has been collected, if the appropriate parameters have been met, the ledger may then serve as the basis for action by an electronic agent issuing the final approval and loan commitment without human intervention.

Various sources suggest that blockchain technologies also may be useful for reliably storing public records, such as real estate or vehicle titles, securities registrations, and health records, to name a few.[115] The focus of this chapter, however, is on the creation, validity, and enforceability of smart contracts and the legal effect of the use of blockchain technology, not on the diversity of potential uses of one or both of these technologies.

[115] Dylan Yaga *et al.*, Draft NISTIR 8202:, Blockchain Technology Overview, NIST (Jan. 24, 2018), https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf (hereinafter "NIST Draft")

II. ESIGN AND THE UETA

In 1997, the Uniform Laws Commission ("ULC") began drafting UETA to bring uniformity to state legislation in the area of electronic records and signatures.[116] The purpose of UETA was to remove legal barriers that prevented the effective use of electronic media by establishing the equivalence of electronic records and signatures to paper records and wet signatures. UETA does not change the substantive provisions of any laws within its scope (*e.g.*, general contracting law). Instead, it generally affects only the medium in which data, including records and signatures, are found.[117]

THUS, WHETHER UETA OR ESIGN APPLIES, THE USE OF ELECTRONIC MEDIA DOES NOT AFFECT THE ENFORCEABILITY OF TRANSACTIONS, WHETHER IN THE FORMATION OF THE RELATIONSHIP OR THE PERFORMANCE OF ITS OBLIGATIONS.

To establish the validity of electronic contracts using electronic records and/or electronic signatures, UETA specifically provides that "a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation."[118] As the Comment states, the section "sets forth the fundamental premise of [UETA]: namely, that the medium in which a record, signature, or contract is created, presented or retained does not affect it's [sic] legal significance."[119]

This validity, however, only applies to the use of electronic records and signatures in connection with a "transaction." A "transaction" is any "action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs."[120] A quick review of the two illustrations above clearly shows that both contract formation and contract performance will involve one or more transactions as so defined. In other words, UETA provides that if a transaction, conducted electronically or not, satisfies the requirements of basic contract law, a contract is formed, and the law will provide a remedy for non-performance or breach of a duty.[121]

Concurrent with the drafting of UETA, the U.S. Congress, at the urging of various industries including high-tech and financial services, decided to act to create a consistent national framework to ensure that electronic signatures and records would be granted the same legal status as traditional (*i.e.*, non-electronic) signatures and paper records.[122] Industry was concerned not only about whether UETA

[116] *See* ESIGN and UETA, *supra* notes 108-109.

[117] UETA, *supra* note 109 at 1.

[118] UETA, *supra* note 109 at §7(b).

[119] *Id.* at cmt. 1.

[120] *Id.* at § 2(16). Note that the defined term "transaction" in UETA differs from the term "transaction" as used by blockchain technologists. The reference by technologists refers to "a recording of a transfer of assets (digital currency, units of inventory, etc.) between parties." NIST Draft, *supra* note 115 at 13. In UETA, the "transaction" is the action between the parties; in the NIST Draft, the "transaction" is the record of that action.

[121] *See* text accompanying n. 10, *et seq.*, *supra*. The Idaho Law Review Symposium, 37 Idaho L. Rev. 233 (2001); Patricia Blumfeld Fry, Introduction to the Uniform Electronic Transactions Act: Principles, Policies, and Provisions, 37 Idaho L. Rev. 237 (2001).

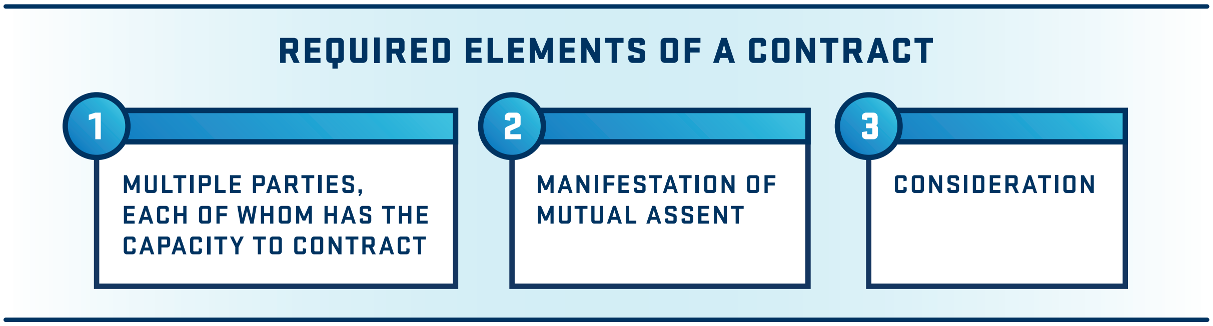
[122] *See* Jeremiah S. Buckley, John P. Kromer, Margo H.K. Tank, R. David Whitaker, The Law of Electronic Signatures, Ch. 4 (Thomson Reuters 2018 ed.).

would ever be adopted nationwide, but also that non-uniform modifications to UETA, as enacted in California, threatened to severely burden commercial use of electronic records and signatures.[123] The Electronic Signatures in Global and National Commerce Act (ESIGN) was the result and was enacted in June of 2000.[124]

Like UETA, ESIGN establishes legal parity between electronic records and signatures and their paper and ink counterparts. Specifically, ESIGN states that for transactions in or affecting interstate or foreign commerce, a signature, contract, or other record cannot be denied legal effect solely because it is in electronic form.[125] Further, a contract related to such transaction cannot be denied legal effect solely because an electronic signature or record was used in its formation.[126] This parity applies to a "transaction," which is "an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons" and includes the sale, lease, exchange, licensing, or other disposition of personal property, services, any combination thereof, or the sale, lease, exchange, or other disposition of an interest in real property or any combination thereof.[127] Thus, whether UETA or ESIGN applies, the use of electronic media does not affect the enforceability of transactions, whether in the formation of the relationship or the performance of its obligations.

III. ELECTRONIC AGENTS AND SMART CONTRACTS

As the Spamco - Widget example illustrates, a commercial transaction may result from the interaction of software code deployed by one or more of the parties to the transaction. The software code may act as the electronic agent of the person deploying it. The question that arises is whether the interaction of one or more electronic agents results in an enforceable contract under U.S. contract law.



REQUIRED ELEMENTS OF A CONTRACT

1 MULTIPLE PARTIES, EACH OF WHOM HAS THE CAPACITY TO CONTRACT

2 MANIFESTATION OF MUTUAL ASSENT

3 CONSIDERATION

A contract is defined in the law as "a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty."[128] Broadly speaking, a contract requires the following elements: (i) multiple parties,[129] each of whom has the capacity to

[123] *Id.*
[124] *See* UETA, *supra* note 109.
[125] *Id.* § 7001(a)(1).
[126] *Id.* § 7001(a)(2).
[127] *Id.* § 7006(13).
[128] Restatement (Second) of Contracts § 1 (1981).
[129] *Id.* § 9.

contract;[130] (ii) manifestation of mutual assent;[131] and (iii) consideration.[132] Of those elements, most relevant to smart contracts is whether there is a manifestation of mutual assent.[133]

The law has long provided that a principal may be bound by the actions of an agent. Agency, briefly, is the relationship whereby a principal grants an agent authority to act on the principal's behalf and subject to the principal's control.[134] An agent can impose contractual liability on the principal for acts done on account of the principal. In general, while there are three distinct bases where the legal consequences of one person's actions are attributable to another, two are relevant for smart contracts: actual authority and apparent authority.[135]

An agent acts with actual authority when the agent reasonably believes, in accordance with the principal's assent to be bound by the agent's actions, that the principal wants the agent to act in such manner.[136] The scope of the agent's actual authority—which includes implied authority as a type of actual authority—can be a complex question and requires that the agent's interpretations and understandings are reasonable. An agent has actual authority to take any action expressly designated or implied by the principal's conduct toward the agent. The agent also may take such actions as are necessary or incidental to achieving the principal's objectives, as the agent reasonably understands the principal's conduct and objectives when the agent determines how to act.[137] An agent acts with apparent authority when a third party believes that the person has authority to act on the principal's behalf and such belief can be traced back to the principal's conduct.[138]

WHETHER USED IN THE PROCESS OF CONTRACT FORMATION OR PERFORMANCE, THE USE OF COMPUTERS TO 'ACT' FOR THE PARTIES IS INHERENT IN THE CONCEPT OF SMART CONTRACTS.

As our illustrations demonstrate, whether used in the process of contract formation or performance, the use of computers to "act" for the parties is inherent in the concept of smart contracts. While some commentators have opined that "the involvement of an autonomous computer in the contract-formation process gives rise to considerable doctrinal difficulties,"[139] these conceptual debates have been rendered

[130] *Id.* § 12.
[131] *Id.* § 17.
[132] *Id.* at Ch. 4. The U.C.C., applicable to commercial transactions, takes a somewhat different approach. It defines a contract as "the total legal obligation that results from the parties' agreement as determined by [the U.C.C.] as supplemented by any other applicable laws." U.C.C. Art. 1, § 1-102(12). An "agreement" is defined as "the bargain of the parties in fact, as found in their language or inferred from other circumstances. … " § 1-102(3). Article 2 specifies that "[a] contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract." § 2-204(1).
[133] This is often colloquially referred to as the "meeting of the minds." As the Restatement makes clear, however, this term is misleading. The requirement is that each of the parties has manifested an intent to be bound. *See* Restatement (Second) of Contracts, *supra* note 12.
[134] Restatement (Third) of Agency § 1.01.
[135] The third, respondent superior, applies to employees acting within the scope of their employment. *See Id.* § 2.04.
[136] *Id.* § 2.01.
[137] *Id.* § 2.02.
[138] *Id.* § 2.03.
[139] Tom Allen & Robin Widdison, Can Computers Make Contracts?, 9 Harv. J.L. & Tech. 25, 34–35 (1996); *see also* Samir Chopra & Laurence

irrelevant when discussing commercial transactions,[140] since both UETA and ESIGN clearly provide that a person may be bound by the operations of an electronic agent or in an automated transaction.

The UETA defines an "electronic agent" as "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual." [141] It goes on to define an "automated transaction" as "a transaction conducted or performed, in whole or in part, by electronic means or electronic records,

in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction."

Building on these definitions, Section 14 of UETA states:

> **SECTION 14. AUTOMATED TRANSACTION. In an automated transaction, the following rules apply:**
>
> (1) A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.
>
> (2) A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.
>
> (3) The terms of the contract are determined by the substantive law applicable to it.[142]

THIS SECTION CONFIRMS THAT CONTRACTS CAN BE FORMED BY MACHINES FUNCTIONING AS ELECTRONIC AGENTS FOR PARTIES TO A TRANSACTION. IT NEGATES ANY CLAIM THAT LACK OF HUMAN INTENT, AT THE TIME OF CONTRACT FORMATION, PREVENTS CONTRACT FORMATION. WHEN MACHINES ARE INVOLVED, THE REQUISITE INTENTION FLOWS FROM THE PROGRAMING AND USE OF THE MACHINE.

As the Comment further elaborates:

> This section confirms that contracts can be formed by machines functioning as electronic agents for parties to a transaction. It negates any claim that lack of human intent, at the time of contract formation, prevents contract formation. When machines are involved, the requisite intention flows

White, Artificial Agents and the Contracting Problem: A Solution via an Agency Analysis, 2009 U. Ill. J.L.Tech. & Policy 363 (2009).

[140] The term "commercial" is used broadly here. *See supra* text accompanying notes 120 and 127.

[141] *Id.* §2(6).

[142] UETA, *supra* note 109 at §14, cmt. 1.

> from the programing and use of the machine. As in other cases, these are salutary provisions consistent with the fundamental purpose of the Act to remove barriers to electronic transactions while leaving the substantive law … unaffected to the greatest extent possible.[143]

ESIGN defines an “electronic agent” somewhat differently than UETA. Under ESIGN, an “electronic agent” is “a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response.”[144] ESIGN provides that:

> “[a] contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.”[145]

As the Senate Report accompanying ESIGN states:

> The bill promotes the use of electronic signatures and provides a consistent and predictable national framework of rules governing the use of electronic signatures. The legislation preempts State law that is inconsistent with UETA, and provides that the electronic records produced in the execution of a digital contract shall not be denied legal effect solely because they are electronic in nature. This legislation also assures that a company will be able to rely on an electronic contract and that another party will not be able to escape their contractual obligations simply because the contract was entered into over the Internet or any other computer network.[146]

THUS, THE LANGUAGE OF BOTH UETA AND ESIGN AND THEIR RESPECTIVE LEGISLATIVE HISTORIES CLEARLY EXPLAIN THAT CONTRACTS AND TRANSACTIONS ENTERED INTO WITH THE ASSISTANCE OR USE OF ELECTRONIC AGENTS ARE ENFORCEABLE AND AS BINDING ON THEIR PRINCIPLES AS IF HUMAN AGENTS HAD BEEN INVOLVED.

Thus, the language of both UETA and of ESIGN and their respective legislative histories clearly explain that contracts and transactions entered into with the assistance or use of electronic agents are enforceable and as binding on their principals as if human agents had been involved.

[143] *Id.* at cmt. 1.

[144] 15 U.S.C. §7006(3). The verbal difference is found solely in the addition of the words “at the time of the action or response” at the end of the ESIGN definition.

[145] *Id.* §7001(h).

[146] S. Rep. No. 106-131 (July 30, 1999).

IV. BLOCKCHAIN BLOCKS AS A SMART CONTRACT, ELECTRONIC RECORD, OR ELECTRONIC SIGNATURE

As discussed above, a blockchain consists of blocks of transaction entries that are cryptographically secured, linked to other blocks through hashes, and then stored in a ledger that is disseminated to multiple computers.[147] The transactions stored in a block may, among many other things, represent computer code programmed to negotiate and enter into agreements, computer code programmed to perform or enforce the obligations the parties under existing agreements (whether formed using electronic agents or not), communications and certifications incident to ongoing commercial relationships, or electronic signatures associated with a transaction. Some blockchain platforms are public (permissionless) blockchains, *i.e.*, anyone with the right software may read and write in them without permission. Others are private (permissioned) blockchains, *i.e.*, they limit participation to specified individuals or companies. Some blockchain platforms, either permissioned or permissionless, are managed by a central entity while in others there is no central authority.[148]

Therefore, smart contracts may operate as an electronic agent, having the effect of forming a legally enforceable contract. The smart contract also may represent code designed to operate as performance of all or part of a contract otherwise formed. Other data may represent links to or entries reflecting required documents, information, or communications between the parties. Blockchain transactions also may constitute, or evidence, electronic signatures. And virtually all transactions stored on a blockchain, and retrievable in perceivable form, constitute an electronic record.

A. RECORDS AND SIGNATURES

The data used to form a smart contract in a blockchain constitutes a "record" as the term is defined in both UETA and ESIGN. UETA defines a "record" as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[149] ESIGN uses identical language.[150] An "electronic record" is "a record created, generated, sent, communicated, received, or stored by electronic means."[151] ESIGN defines an "electronic record" in nearly identical language, *i.e.*, "the term 'electronic record' means a contract or other record created, generated, sent, communicated, received, or stored by electronic means."[152] Therefore, so long as it is retrievable in perceivable form, the record of a transaction stored in a blockchain is a "record" and an "electronic record" under both UETA and ESIGN.[153]

UETA and ESIGN also provide a consistent definition of "electronic signature" that encompasses the use of a blockchain. As defined in UETA, an "electronic signature" is "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[154] The ESIGN definition is virtually identical:

[147] *See supra* text accompanying notes 112-113.

[148] *See* NIST Draft, *supra* note 115.

[149] UETA, *supra* note 109 at § 2(13). As the Reporter's Comment notes, the definition is designed to "embrace all means of communicating or storing information except human memory."

[150] 15 U.S.C. § 7006(9).

[151] UETA, *supra* note 109 at § 2(7).

[152] 15 U.S.C. § 7006(4).

[153] Christina L. Kunz, The Definitional Hub of E-Commerce: "Record," 45 Idaho L. Rev. 399 (2009).

[154] UETA, *supra* note 109 at § 2(8).

> (T)he term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.[155]

A blockchain entry either may constitute a signature itself as the record of a "process" logically associated with a record or it may contain evidence that such a process was completed in another environment, or it may contain a sound or symbol that constitutes a signature and is merely recorded on a blockchain. In any of these instances, so long as the purported signer had the requisite intent, and the signature is either attached to or logically associated with the signed record, then the signature is an electronic signature.

B. BLOCKCHAIN AS A SECURITY PROCEDURE

While ESIGN is silent on the subject, UETA contains provisions recognizing the impact of security procedures operating on electronic records or signatures. UETA defines a "security procedure" as a:

> [P]rocedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.[156]

As noted above, a blockchain involves blocks of cryptographically secured entries, linked together, and stored in a distributed ledger. The encryption, the hashing, and the disseminated nature of the ledger render the transaction records immutable.[157] UETA does not accord security procedures "operative effect, through presumptions or otherwise… [T]he use of security procedures is simply one method for proving the source or content of an electronic record or signature."[158]

The Act goes on to provide, in Section 9, that:

> An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.[159]

It further provides, in Section 10, that:

> If a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply:
>
> (1) If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming

[155] 15 U.S.C. § 7006(5).
[156] UETA, *supra* note 109 at § 2(14).
[157] *See supra* text accompanying note 112 *et seq.*
[158] UETA § 2 Reporter's Comment 11.
[159] *Id.* § 9(a).

> party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record … .
>
> (3) If … paragraph (1) [does not apply], the change or error has the effect provided by other law, including the law of mistake, and the parties' contract, if any.[160]

Thus, under UETA, the fact that the entries are stored on a blockchain is given special weight in two circumstances: first, where the technology provides evidence of the signer's identity, and second, where the technology is designed to detect a particular type of change or error, and one of the parties fails to use the technology as agreed and the error goes undetected as a result.

V. DETERMINING THE LAW APPLICABLE TO A SMART CONTRACT OR TRANSACTIONS RECORDED IN A BLOCKCHAIN

This chapter demonstrates that transaction records stored on a blockchain constitute an "electronic record" under either state-enacted versions of UETA or the federal ESIGN statute and that, if used with the intent to sign, can constitute an "electronic signature" under the same statutes. Our more extended discussion further demonstrates that under these statutes, records of transactions stored on a blockchain or another electronic format may constitute an enforceable contract. Under both statutory regimes, the use of an automated agent does not raise new questions about the enforceability of such contracts. It is important to note that the conclusion that either or both UETA or ESIGN are applicable to the creation of a smart legal contract or the use of a blockchain as part of a transaction does not complete the analysis of governing law. Both ESIGN and UETA are designed to ensure that electronically-based transactions are on a par with paper-based transactions, no better and no worse in the eyes of the law. UETA generally does not change the substantive provisions of laws within its scope, but it does provide that electronic records and electronic signatures are to be treated on par with those on paper media. As the Prefatory Note to UETA explains:

> With the advent of electronic means of communication and information transfer, business models and methods for doing business have evolved to take advantage of the speed, efficiencies, and cost benefits of electronic technologies. . . .
>
> It is important to understand that the purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures. It is NOT a general contracting statute—the substantive rules of contracts remain unaffected by UETA. . . .
>
> The Act's treatment of records and signatures demonstrates best the minimalist approach that has been adopted. Whether a record is attributed to a person is left to law outside this Act. Whether an electronic signature has any effect is left to the surrounding circumstances and other law. These provisions are salutary directives to assure that records and signatures will be treated in the same manner, under currently existing law, as written records and manual signatures.[161]

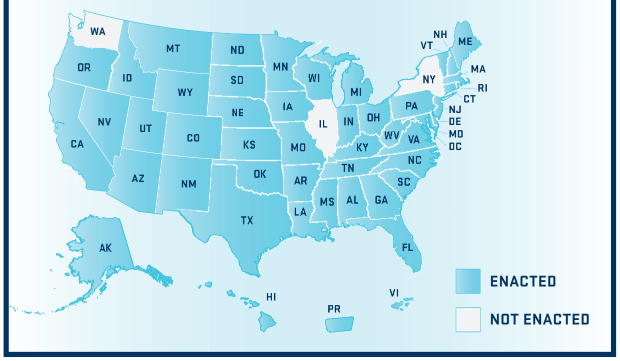
[160] UETA, *supra* note 109 at § 10.
[161] UETA, *supra* note 109 at Prefatory Note.

BOTH ESIGN AND UETA ARE DESIGNED TO ENSURE THAT ELECTRONICALLY-BASED TRANSACTIONS ARE ON A PAR WITH PAPER-BASED TRANSACTIONS, NO BETTER AND NO WORSE IN THE EYES OF THE LAW.

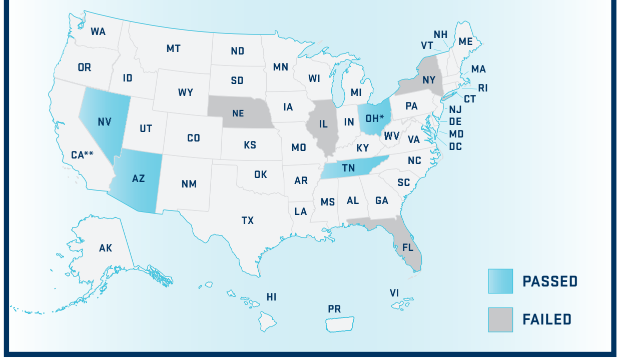
ESIGN takes the same approach, specifying that the use of electronic media does not affect or interfere with the enforceability of electronic transactions without displacing otherwise applicable law.[162]

If the parties' conduct is within the scope of a state's version of the Uniform Commercial Code, that law will determine whether a contract exists and the scope and nature of the obligations arising from that contract.[163] For other contracts, the Restatement (Second) of Contracts generally provides guidance to state courts to determine whether a contract exists and the scope and nature of the obligations arising from that contract.[164] Various and sundry federal or state laws may govern specific types of contracts, such as those with consumers,[165] or specific types of transactions, such as transfers of securities or real estate.[166] The use of a smart contract or blockchain may have an impact on the evidence needed or available to establish whether an agreement was reached and its obligations fulfilled.

UETA ENACTMENT STATUS



SMART CONTRACT LEGISLATION



*Ohio has 1 bill on smart contracts.

**California introduced a bill, but was amended to focus on blockchain working group.

[162] 15 U.S.C. 7001(a) (2000).

[163] *See supra* note 117.

[164] *See supra* text accompanying notes 128-132.

[165] For example, the Truth-in-Lending Act, 15 U.S.C. 1601, *et seq.*, imposes liability on consumer lenders which fail to provide various disclosures and protections in consumer credit transactions.

[166] *See, e.g.*, Traynum v. Scavens, 416 S.C. 197 (S.Car. 2016), in which the court ruled that an offer of underinsured motorist coverage on an insurer's website satisfied legal requirements.

VI. CONCLUSION

Blockchain platforms may constitute or store electronic records, electronic signatures, and computer code designed to function as electronic agents, and thus may be used to evidence, or give effect to, electronic or smart legal contracts. The UETA and the federal ESIGN Act provide the legal framework for smart contracts and blockchain use. Both laws were designed and intended by their drafters to assure that the use of electronic media would not affect the enforceability of commercial transactions. Neither legislative regime was intended to alter the laws governing commercial transactions, beyond assuring that the use of electronic media and technologies was not interpreted as impairing or altering those existing legal regimes. This was accomplished by recognizing that electronic records are records, electronic signatures are signatures, and that contracts may be formed and performed using electronic technologies, with or without human intervention.

CHAPTER 3: U.C.C. AND STATE LAW ISSUES IN SMART CONTRACTS

Jenny Cieplak[167]

Depending on the substance of a smart legal contract, many different state laws may govern how contract rights are enforced. For instance, laws related to the sale of insurance in the case of insurance contracts, laws related to consumer finance and protection in the case of business-to-consumer contracts, and laws governing data privacy in the case of almost every transaction where the identity of the parties is known, and the transaction is not completely anonymous. Of course, a single chapter in a white paper cannot cover the entire spectrum of state laws or fact patterns in which they may apply, and this chapter does not aim to do that. Instead, this chapter considers a threshold issue regarding state law and the Uniform Commercial Code ("U.C.C.")—namely, how both blockchain-based[168] and tokenized[169] assets should be characterized for purposes of Article 9 of the U.C.C.

Chapter 3 first considers whether blockchains and smart contracts may be used to represent security interests. This section analyzes the different Article 9 categories for assets that may apply to blockchain-based assets. It also provides an overview of perfection of security interests in various asset types and how those rules may apply to a blockchain and tokenized assets (assets that live outside the blockchain). Second, this chapter considers enforcement issues for smart contracts. This section addresses the issues of location of the assets, whether enforcement is possible on a blockchain, and the possible effect of location of a centralized authority or intermediary who holds blockchain-based assets. As set forth below, in the absence of further guidance as the blockchain-based economy grows, the safest course for a party to a smart contract is to ensure those assets are either deposited into the smart contract itself, or with a third-party provider who is willing to provide assistance with enforcement.

VII. CAN A BLOCKCHAIN BE USED TO REPRESENT SECURITY INTERESTS?

For many U.C.C. practitioners, the concept of security interests is of primary importance. If a party desires to obtain financing through a loan or through the issuance of debt securities, the provider of financing will wish to have a security interest in some or all of the debtor's assets. In the case of both blockchain-based assets (*i.e.*, those assets that exist solely on a blockchain, such as bitcoin and other

[167] Jenny Cieplak is a FinTech attorney and the head of Crowell & Moring, LLP's distributed ledger initiative. Ms. Cieplak is known as a thought-leader on blockchain and distributed ledger technology in the financial space, and has counseled clients in connection with the development and implementation of blockchain solutions.

[168] An asset that consists solely of a token on a blockchain. *See* definition of "blockchain-based asset" in the Lexicon.

[169] An asset that consists of intangible or tangible property apart from a blockchain, such as real or chattel property or a legal interest in some asset, but which is represented by a token on a blockchain. *See* definition of "tokenized asset" in the Lexicon.

virtual currencies) and tokenized assets (*i.e.*, assets that have a separate existence, such as real property or fine art whose ownership is tracked on a blockchain), the financing provider will want to be familiar with how the principles of Article 9 of the U.C.C. apply to the assets. The utility of the assets will increase if owners are able to use them as collateral in financing transactions.

As a brief reminder of Article 9 principles, in order to obtain a security interest in an asset, the debtor must have rights in the collateral, a financing provider must have given value to the debtor, and the security interest must be set forth in an agreement containing a description of the collateral that is authenticated by the debtor. This agreement can be in written or electronic form, and it can be authenticated through electronic means—theoretically, including through public key/private key signature. Thus, a party should be able to obtain and document a security interest via a smart contract, as theoretically the smart contract would identify the blockchain-based asset or tokenized asset that constitutes the collateral, and it would be authenticated by the debtor through its private key signature.[170]

There is, however, another step that financing providers typically take that gives them additional protection in the collateral—that of perfecting their security interest. A perfected security interest allows the financing provider to have priority over the relevant collateral in the event the debtor does not have sufficient assets to pay all of its debts. Conversely, an unperfected security interest may be subordinated to other creditors of the debtor. Perfection can be obtained in a number of ways – by filing with the relevant Secretary of State's office, by the secured party's entering into a control agreement with a third party that maintains custody of the collateral, or by the secured party's taking possession of the collateral. The best way to perfect a security interest is determined by the Article 9 "category" into which an asset falls. Therefore, it is first necessary to categorize blockchain-based assets and tokenized assets for U.C.C. Article 9 purposes.

Perfection is generally governed by the law of the state in which the debtor is located.[171] However, the location of an asset is sometimes relevant as well. U.C.C. Section 9-301 provides that the law of the state in which the asset is located can govern perfection by possession, and also governs the effect of perfection or nonperfection and the priority of a nonpossessory security interest (such as perfection through control). Given that all states have implemented the security interest provisions of the U.C.C. with only some subtle differences, this section will ignore differences between the states. The following section considers how parties can determine which state's law governs for the cases where it is relevant.

A. CATEGORIZING BLOCKCHAIN-BASED ASSETS FOR ARTICLE 9 PURPOSES

The same asset can be categorized differently for different purposes. For example, some government agencies are treating virtual currencies as money, such as the Financial Crimes Enforcement Network ("FinCEN"). Others, such as the Internal Revenue Service ("IRS")/Commodity Futures Trading Commission ("CFTC"), are treating virtual currencies as property or as a commodity. No government agency has made an announcement regarding the treatment of virtual currencies or other blockchain-

[170] *See* U.C.C. § 9-203 (2010).
[171] U.C.C. § 9-301 (2010).

based assets for U.C.C. Article 9 purposes. An examination of the relevant categories is therefore necessary. Most categories can be eliminated immediately as they relate to physical assets. Several categories deserve a closer look, including investment property and general intangibles.

1. BLOCKCHAIN-BASED ASSETS ARE NOT: MONEY, DEPOSIT ACCOUNTS AND COMMODITY ACCOUNTS

The Article 9 category of "money" is defined as "a medium of exchange currently authorized or adopted by a domestic or foreign government." Although FinCEN has stated that virtual currencies are to be treated as "currencies" for anti-money laundering laws, this does not constitute adoption of virtual currencies as a medium of exchange. If some government were to adopt a virtual currency as its "currency," or more likely to issue its own virtual currency, then the analysis would differ. Although the U.C.C. definition of "money" has traditionally only been applied to physical currency, the statute does not seem to exclude digital manifestations of money held directly by the owner.

Currency held in an account with a depository institution is treated differently, which may be because such currency cannot really be said to be "held" by the beneficiary at all—instead, it represents a claim on the depository institution in which the account is held. The U.C.C. term "deposit account" applies here, and it is defined generally as "a demand, time, savings, passbook or similar account maintained with a bank."

While at first it might seem possible to shoehorn a virtual currency wallet maintained with a wallet provider into this definition, the U.C.C. also includes a specific definition of "bank" that eliminates entities not engaged in the business of banking. Since most wallet providers would hardly wish to hold themselves out as engaged in banking, it is unlikely that this category would apply. In addition, the definition of "deposit account" is generally considered to relate only to accounts for "money," and accounts holding "investment property" are specifically excluded from the definition.[172]

Since the CFTC has stated that virtual currencies are commodities, one would think it possible that a blockchain-based asset could fall into the "commodity contract" or "commodity account" categories—however, these categories are limited to futures and derivatives accounts, and not to situations where one entity simply holds commodities for the account of another.

2. INVESTMENT PROPERTY: A POSSIBILITY

The category of "investment property" holds some promise for blockchain-based assets. This category includes securities and commodity contracts, as well as the more amorphous term "security entitlements."

[172] *See* U.C.C. § 9-102(a)(29) (2010).

Interestingly, although the Securities and Exchange Commission ("SEC") has stated that some blockchain-based assets constitute "securities," it is unclear whether interests in a decentralized autonomous organization ("DAO") can be considered "securities" for U.C.C. purposes. As defined in the U.C.C., a "security" is "an obligation of an issuer or a share, participation, or other interest in an issuer or in property or an enterprise of an issuer." It is not clear whether a token such as the DAO token would be considered a security for this purpose, since the DAO did not actually have an "issuer," and in many cases blockchain-based assets do not represent an obligation of an issuer but rather permit the holder to access some functionality on the blockchain with respect to which they are issued.

However, just because an asset does not constitute a "security" for U.C.C. purposes does not mean it cannot be treated similarly to a security. "Security entitlements" are treated in the same manner as securities for Article 9 purposes.

A "security entitlement" is defined as "the rights of an entitlement holder with respect to a financial asset."[173] The definition of "financial asset" is quite broad and can encompass "any property that is held by a securities intermediary for another person in a securities account if the securities intermediary has expressly agreed with the other person that the property is to be treated as a financial asset under" Article 8 of the U.C.C.[174] This definition is somewhat circular and becomes more circular still when one considers that the definition of "securities intermediary" is "a person, including a bank or broker, that in the ordinary course of its business maintains securities accounts for others and is acting in that capacity,"[175] and that a "securities account" is basically "an account to which a financial asset is or may be credited."[176]

The conclusion to be drawn from all of this is that, if a blockchain-based asset is held by a third-party wallet provider, then, if that wallet provider so agrees, the asset can be treated as a financial asset, and thus as a security entitlement, and thus as investment property.

3. GENERAL INTANGIBLES: THE CATCHALL CATEGORY

If an asset is not covered by any of the other U.C.C. categories, it will most likely be considered a general intangible. The definition of "general intangible" is in fact a reference to what a general intangible is not—that is, if an asset constitutes personal property (*i.e.*, any property that is not real property), and it does not fall into any of the other named categories, then it is a general intangible.[177] Domain names, software, and patents are typical general intangibles, as are contract rights.

[173] U.C.C. §8-102(a)(17) (1994).
[174] U.C.C. §8-102(a)(9) (1994).
[175] U.C.C. §8-102(a)(14) (1994).
[176] U.C.C. §8-501(a) (1994).
[177] Hansen & Boehm, *supra* note 104.

However, blockchain-based assets differ in important ways from most other types of general intangibles. Unlike domain names, software, patents and contract rights, blockchain-based assets (at least assets maintained on a UXTO-type blockchain) are designed to be fungible.[178] This distinction has an important impact on how security interests in blockchain-based assets will be treated if such assets are considered general intangibles versus another type of property.

B. PERFECTION OF SECURITY INTERESTS IN VARIOUS ASSET TYPES

1. PERFECTING SECURITY INTERESTS IN MONEY

A security interest in "money" may only be perfected by the secured party's taking possession of the money.[179] However, the U.C.C. lacks a definition of "possession"—the term originally included only tangible items (including physical cash as well as other negotiable documents). Most intangible items (such as general intangibles, uncertificated securities, and deposit accounts) cannot be perfected by possession at all because there is no evidentiary way to determine who has "possession" of those items without referring to another method of perfecting a security interests, such as filing with the appropriate Secretary of State or establishing a control relationship with an intermediary.

For blockchain-based assets, there is a way to determine who has possession—by determining who has possession of the private key used to store those assets. Thus, if blockchain-based assets such as virtual currencies are ever considered "money" for purposes of the U.C.C., it would be possible to perfect a security interest in such assets through possession. However, granting a secured party possession of blockchain-based assets, like granting a secured party possession of money, is not very practical if the debtor is concerned that the secured party may abscond with the assets. Requiring two-key authentication for transactions in blockchain-based assets that are subject to a security interest may be a possibility that satisfies this concern, although it is not clear whether this would constitute "possession" for U.C.C. purposes.

Allowing the secured party to perfect its interest by possession is also impractical if the debtor wants to retain use of those assets during the term of the security interest. While perfection by possession is sometimes used for items such as certificated securities that are not freely marketable, one of the values of blockchain-based assets lies in their liquidity. A holder of bitcoin, for example, might want to trade in virtual currency markets instead of holding those bitcoin long-term, while at the same time using his or her virtual currency holdings as collateral for a loan. Luckily for that holder, there is another way for a secured party to perfect its interest in blockchain-based assets, as long as those assets are held through an intermediary that is willing to cooperate.

[178] While many in the cryptocurrency world take the view that bitcoin and other UXTO-based virtual currencies are not truly fungible because transactions can be traced, and because buyers are sometimes willing to overpay for coins from newly-minted blocks, a bitcoin itself cannot truly be traced. In fact, individual bitcoin should be thought of as more abstractions than real coins. This is because the Bitcoin blockchain, and others like it, are really a ledger of transactions and not a ledger of coin ownership. An example is perhaps the best explanation here: The ledger shows the number of bitcoin in each wallet, and transactions between wallets can be traced. So, if Alice sends 10 bitcoin to Bob, and Carol also sends 10 bitcoin to Bob, Bob is shown as having 20 bitcoin in his wallet. If Bob then sends 10 bitcoin to Dana, it is impossible to tell whether Bob sent her the 10 bitcoin from Alice, the 10 bitcoin from Carol, or a combination thereof.

[179] U.C.C. § 9-312(b)(3) (2010).

2. PERFECTING SECURITY INTERESTS IN DEPOSIT ACCOUNTS AND FINANCIAL ASSETS

Deposit accounts and financial assets are treated quite similarly under the U.C.C., as they have much in common. In particular, deposit accounts and financial assets are held not by physical possession but through an intermediary. Thus, the U.C.C. provides for a type of perfection in security interests known as "control." Unlike "possession," the means for a party to obtain "control" are clearly set out in the statute. All that is needed is for the depository institution (with respect to deposit accounts)[180] or intermediary (with respect to financial assets)[181] to agree in writing with the debtor and the secured party as to the existence of the security interest.[182]

The debtor may or may not retain the authority to direct the disposition of the assets in the account until such time as the secured party forecloses on the assets.[183] Of course, in order for a lender to be comfortable allowing a borrower to have freedom to move assets to and from accounts, that lender will want to retain other controls and visibility into the borrower's operations. For blockchain-based assets today, especially for use in smart contracts where the parties may not have an ongoing relationship, it is unlikely that the secured party will want the grantor of the security interest to retain this type of control — but as blockchain-based assets become more widely accepted in the business community, borrowers may want to take advantage of this freedom.

Another useful aspect of using the "control" method of perfecting a security interest in a blockchain-based asset is that the law that governs whether "control" has in fact been obtained is the law of the depositary institution or securities intermediary's jurisdiction.[184] This allows parties to sidestep the issue of where the asset is located, which typically dictates the law governing perfection by possession.[185]

3. PERFECTING SECURITY INTERESTS IN GENERAL INTANGIBLES

If a blockchain-based asset is treated as a general intangible, the only way to perfect a security interest in that asset is by filing with the Secretary of State's office. The relevant filing office is determined by the location of the debtor (for U.S. legal entities that is the jurisdiction in which the entity was formed). But the filing regime may not be practical for blockchain-based assets. First, such assets are designed to be extremely liquid compared to intangibles such as patents and rights in tax refunds, both of which are considered general intangibles. While perhaps a filing could be made with respect to "all bitcoin owned by ABC, Inc.," this does not help the parties to a pseudonymous smart contract. A filing for "all bitcoin associated with public key X" is also impractical as the amount of bitcoin associated with that public key could change rapidly, and the user could move assets from one address to another.

[180] U.C.C. § 9-104 (2010).

[181] U.C.C. § 9-106 (2010); U.C.C. § 8-106 (1994).

[182] For investment property, you can perfect by filing, U.C.C. § 9-312(a) (2010), but that will be subordinate to a perfection by control (U.C.C. § 9-328) (2010).

[183] U.C.C. § 9-104(b) (2010)

[184] *See* U.C.C. § 9-305 (2010) (discussing investment property); *see also* U.C.C. § 9-304 (2010) (discussing deposit accounts).

[185] U.C.C. § 9-301 (2010).

In addition to the practical limitations, there is a legal concern with classifying extremely liquid assets such as virtual currencies as general intangibles. When a secured party has perfected a security interest in a general intangible, and then that general intangible is sold to a subsequent buyer, the subsequent buyer takes the general intangible subject to the lien unless it has been specifically released. In other words, a buyer of general intangibles must be sure to do a search of liens filed in the relevant Secretary of State's offices in order to be sure that the general intangibles it is purchasing are not subject to any liens.

This "buyer-beware" system may work for general intangibles like contract rights that are not freely traded, since a buyer should be able to trace the ownership history of the right and determine the appropriate Secretary of State's office in which to run searches. But for assets such as bitcoin which pass through thousands of owners, not only is such a search impracticable, it may be impossible. Since a UXTO-based blockchain tracks transactions and account balances as opposed to actual coins, if blockchain-based assets are treated as general intangibles, it may be impossible to tell whether a blockchain-based asset was ever subject to a security interest.

C. SECURITY INTERESTS IN TOKENIZED ASSETS

One use case that companies are considering is using blockchains to record ownership of assets that exist outside the blockchain—that is, tokenized assets. For example, Everledger has created a system for tracking diamonds using the technology. Theoretically, a sale of a diamond tracked using Everledger's technology would be accomplished through a transfer of title on the blockchain-based record, which would represent a transfer in the "real world." Such a transfer would certainly be admissible evidence of the transfer in any court.

Imposing a security interest through a smart contract on a blockchain such as Everledger's is a different story. Diamonds, like the vast majority of movable physical property, constitute "goods" for purposes of the U.C.C. And the only way that a security interest in goods can be perfected is through making a filing with the appropriate Secretary of State's office. Notating a security interest through a smart contract on a distributed ledger, while it will be accepted as evidence of the security interest, will not constitute perfection. And a party with an unperfected security interest, regardless of the fact that such party may receive temporary ownership through the automatic execution of the smart contract, is subject to having its title revoked by a court in the event another party has a perfected security interest.

Of course, this is not to say that parties seeking to obtain a security interest in a tokenized asset should disregard the token system entirely. Any practical attorney will encourage clients to run a search on the relevant ledger to ensure that no party has a competing claim to the asset, and to obtain a security interest in any token representing ownership or otherwise indicate the security interest on the ledger. But such a process makes financing more cumbersome, not less.

EXAMPLES OF TOKENIZED ASSETS

There is, however, a way to combine the filing of a U.C.C. security interest with the filing of a smart contract on a blockchain system without requiring any change in the law. While some states specify a paper process and others permit online filing using legacy systems, there is nothing in the U.C.C. that requires any specific medium for indication of security interests. Thus, it is possible for a state to utilize a blockchain-based system—even to utilize a blockchain-based system operated by a third party as long as the state filing office has its operations on that system. While U.C.C. § 9-501 seems to specify that security interest filings must be made with an office of the state, there is nothing preventing a state from operating a node on a blockchain and designating that blockchain as the means through which statements must be filed. A blockchain with a user-friendly interface would be just as accessible as the online filing systems used by many states currently. And such a system could be interoperable with other blockchain systems, allowing parties greater freedom in the systems they want to use.

VIII. ENFORCEMENT ISSUES: WHERE IS A BLOCKCHAIN-BASED ASSET LOCATED?

As discussed above, in some cases the location of an asset determines which state's law governs perfection of a security interest, or the effect of perfection. In addition, a holder of a security interest may wish to foreclose on that interest and may need access to the courts in order to do so. In both secured loan transactions and other types of smart legal contracts, there are scenarios imaginable where a smart contract does not properly execute and the parties have a dispute that requires access to the courts. Errors in code could prevent a transfer or could cause the incorrect amount of virtual currency to be transferred. Unless the smart contract requires a 100% deposit upfront, the holder of virtual currency could drain their account prior to the payment date. A third party could have a conflicting claim on the virtual currency, whether through a smart legal contract or otherwise. Or there could be a dispute as to whether payment is actually owed, especially for more complex types of smart legal contracts such as contracts for services. The appropriate court to exercise a judgment on an asset is typically the court in which the asset is located.

A. LOCATION OF INTANGIBLE ASSETS GENERALLY

A threshold question is whether a court can reach a blockchain-based asset to satisfy a judgment, and which is the appropriate court to do so. Whether a blockchain-based asset constitutes a property right that can be used by a court to satisfy a judgment is a question of state law, and the initial question must be one of where a blockchain-based asset is located in order to determine which state's law to apply — or, indeed, if a blockchain-based asset is located anywhere.[186]

Although intangible assets cannot be said to have a physical location, many courts take the view that intangible assets are located in, or at least are subject to the laws of, the jurisdiction in which the central register of such asset is maintained.[187] The prototypical example of such intangible property in cyberspace is the domain name, which is an intangible asset that could be said to be "located" anywhere a computer can access it. However, the allocation of domain names is controlled by a registrar such as Network Solutions Inc. ("NSI"), which is based in Virginia, and it is generally the consensus that a domain name is technically "located" in the jurisdiction where the registrar is located. In *Network Solutions Inc. v. Umbro*, the Virginia Supreme Court acknowledged that domain names registered with NSI were intangible property located in Virginia—although that court also found that because of the specifics of Virginia's garnishment statue, Umbro was unable to garnish the domain names at issue. The U.S. Anticybersquatting Consumer Protection Act similarly provides that a domain name is "located" at the location of its registrar.[188]

B. LOCATION OF ASSETS ON A DISTRIBUTED NETWORK SUCH AS A BLOCKCHAIN

The traditional logic set forth above to determine the location of intangible assets is not necessarily the best fit for blockchain. One of the central tenets of bitcoin and other public blockchain virtual currencies is that there is no single entity or group that controls ownership or registration of blockchain-based assets. Public blockchains exist nowhere but on the computers of all those who have downloaded the public blockchain, and transactions are propagated throughout a public blockchain network without regard to any network hierarchy. Blockchain-based assets on a public blockchain are less analogous to domain names, and more analogous to trade secrets or unregistered copyrights, which similarly have no central repository or registration authority. Even though intellectual property such as patents can be registered with the U.S. government, the Supreme Court going back to 1881 stated that patents and copyrights cannot exist in any particular state, or in fact anywhere. Thus, the Court held that there could be no execution of judgment against a patent because the patent is not within any court's jurisdiction.[189]

[186] Part 2, Section B, *infra*, will address the issue of "tokenized" assets – that is, assets that have an existence apart from the blockchain but that are tracked through blockchain tokens or applications, such as fine art.

[187] *See* Thomas R. Lee, In Rem Jurisdiction in Cyberspace, 75 Wash. L. Rev 97, 127-28 (2000).

[188] 15 U.S.C. § 1125(d)(2) (2012).

[189] *See* generally, Ager v. Murray, 105 U.S. 126 (1881); *see also* Juliet M. Moringiello, Seizing Domain Names to Enforce Judgments: Looking Back to the Future, 39, SSRN (2003), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1270651.

C. IS ENFORCEMENT POSSIBLE ON THE BLOCKCHAIN?

An additional practical consideration comes into play when considering assets located on Bitcoin and similar public blockchains. The only way to transfer assets on the Bitcoin blockchain from a specific wallet is to utilize the private key associated with that wallet. This means that even a party with a perfected security interest in bitcoin or another blockchain-based asset, which typically under the Uniform Commercial Code can be foreclosed on through "self-help" without resorting to a judicial remedy, cannot foreclose on the asset unless the applicable smart contract code makes the transfer possible.

Even the U.S. government has had difficulties obtaining bitcoin in forfeiture cases—unless it has access to the hardware on which the wallet and the applicable private key is stored. In *U.S. vs 50.44 Bitcoin*, the court did not have to reach a conclusion regarding the location of the bitcoin at issue, or even whether any court could force a transfer of the bitcoin through technological means, because the holder of the bitcoin appears to have voluntarily transferred them to the government. Although for such a forfeiture case, the complaint is supposed to state the basis for in rem jurisdiction over the property subject to forfeiture,[190] the verified complaint for the case does not refer to jurisdictional issues at all other than to say that the personal computer on which the relevant bitcoin wallet was stored was located in Maryland. And since the case was decided on a default judgment, it appears that jurisdictional issues were not raised.

The FBI also managed to seize a large sum of cryptocurrency from Ross Ulbricht, the creator of the Silk Road, an online marketplace for drugs and other illegal activities. However, the FBI again accomplished this seizure through physical means—by seizing his laptop along with servers used to run the Silk Road itself.[191] And in a more recent case, law enforcement agents seized cryptocurrency assets held by Alexandre Cazes, the creator of a successor criminal enterprise site known as Alpha Bay, when it seized his unencrypted computer which listed the wallet addresses and private keys corresponding to those assets.[192]

However, there are other ways parties can gain certainty over whether a court can enforce a judgment over a blockchain-based asset. Participating in a private blockchain with a centralized authority, or utilizing a third-party intermediary to hold blockchain-based assets, may give parties to smart legal contracts more reliability—although at the expense of the decentralization that many blockchain proponents desire.

[190] Fed. R. Civ. P. G.

[191] Partial Judgment by Default and Order of Forfeiture, United States v. Ross William Ulbrich, No. 13 Civ. 6919 (JPO) (S.D.N.Y 2014).

[192] Verified Complaint for Forfeiture In Rem, United States v. Alexandre Cazes, 1:17-at-00557, (E.D.Cal. 2017).

D. BLOCKCHAIN-BASED ASSETS HELD THROUGH AN INTERMEDIARY, OR WHERE THERE IS A CENTRAL AUTHORITY

Blockchain-based assets on a network with a centralized authority, or held through a known wallet provider, will provide more avenues for access. By analogizing to the domain names example, one could say that in the case of blockchain-based assets held through a known wallet provider, those assets are held in the jurisdiction where the wallet provider is located. This is a question of where the wallet provider is located, not where its servers are located, again referring to the example of NSI. Although NSI has servers and backup sites in many locations, the “location” of domain names registered by it is deemed to be the location of its principal place of business. Assets held through a centrally-managed blockchain, or even a blockchain that has only one entity that validates transactions, could be treated similarly.

In a real-world example, the U.S. government has seized assets held through Coinbase, a well-known provider of bitcoin wallet services.[193] However, it appears that Coinbase has not contested these forfeiture actions, and so there is little case law on the issue of whether assets held through Coinbase or another wallet hosting provider can be seized through action in a jurisdiction where the wallet provider itself is not located.

IX. CONCLUSION: A PATH FORWARD

The safest method for a party to a smart legal contract receives the blockchain-based assets to which it is entitled is to ensure that those assets are either deposited into the smart contract itself, or with a third-party provider that is willing to provide assistance with enforcement. As the blockchain-based economy grows, however, more guidance may be needed around how smart contracts can be practically enforced, especially where security interests are at issue. For example, rather than leaving blockchain-based assets in the catchall category of general intangibles, it may be preferable for the drafters of the U.C.C. to contemplate an entirely new category of asset, which would be treated similar to “money,” but which would allow the use of dual signatures to represent “possession” in new ways. Alternatively, it could be clarified that the operator of a blockchain network can be treated as a “securities intermediary” so that assets on the network can be characterized as “financial assets.” As more and more jurisdictions are exploring the use of blockchain technology it can be expected that additional issues will arise where old paradigms must be replaced with new thinking.

[193] William Suberg, KYC Dilemma: US Secret Service Seizes $13k from Coinbase Customer, Bitcoin.com (Jul. 23, 2016), https://news.bitcoin.com/us-secret-service-seizes-coinbase/.

CHAMBER OF
DIGITAL
COMMERCE

DIGITALCHAMBER.ORG | @DIGITALCHAMBER

SMART CONTRACTS: Is the Law Ready?

D9 | SEP. 18