CARDOZO BLOCKCHAIN PROJECT

Research Report #2

“SMART CONTRACTS” & LEGAL ENFORCEABILITY

October 16, 2018

About

The Cardozo Blockchain Project is an initiative from Cardozo Law School to explore the legal issues and challenges related to blockchain technology. The project is directed by Aaron Wright. To learn more, please visit our website: https://cardozo.yu.edu/programscenters/blockchain-project or send an email to aaron.wright@yu.edu.

Supporters

The Cardozo Blockchain Project would like to thank the following individuals (acting solely in their personal capacity) for their substantial input, guidance and support on the below report.

DLx Law LLP
Brian Ray
Susan Joseph
Stuart D. Levi
Patrick Berarducci

Thousands of years ago, written contracts first appeared in Mesopotamia, with small cuneiform triangles hammered into clay tablets. These contracts were fairly sophisticated, memorializing basic credit agreements, partnership arrangements, as well as labor, sales, and rental agreements.[1] Since these first recorded contracts, the tools used to create written contracts have undergone considerable change. We no longer enter into agreements memorialized in clay; paper and more recently electronic agreements serve as the primary medium for the expression of commercial arrangements.

Many argue that blockchains could foster an evolution in how legal agreements are created and executed, supporting a new generation of electronic contracts. Blockchain networks and computer programs called "smart contracts" could enable parties to memorialize all or parts of legal agreements. By using this technology, contracting parties would gain the ability to create arrangements that are hard to modify, dynamic, and potentially less ambiguous than traditional legal contracts.

This report assumes such a future comes to pass and examines how blockchain technology fits within the current common law and U.S. electronic contracting statutes, analyzing whether smart contracts can be used to create enforceable legal agreements. As outlined below, we explain why current U.S. law largely accommodates the use of smart contracts to create binding and enforceable agreements. We conclude the report by analyzing whether additional state and federal legislation is necessary to support this new emerging technology, finding that current iterations of state law, designed to accommodate blockchain technology, may not be necessary, with limited exceptions.

The report unfolds in three parts. Part I provides a brief overview of blockchain technology and smart contracts, with an assumption that the reader has limited familiarity with the underlying technology. Part II explores whether legal agreements relying on blockchain technology will be deemed enforceable. Finally, Part III evaluates whether additional legislation is necessary to accommodate electronic contracting involving blockchain-based smart contracts.

I. Overview of Blockchain Technology and Smart Contracts

The potential for blockchain technology extends far beyond payment systems such as Bitcoin. Blockchain technology has the potential to anchor a new generation of electronic contracts that offer broader capabilities than existing written agreements. In this section, we briefly unpack how blockchain technology works and introduce the related concept of "smart contracts."

[1] *See*, *e.g.*, Paul Halsall, Ancient History Sourcebook: A Collection of Contracts from Mesopotamia, c. 2300 - 428 BCE, in Internet Ancient History Sourcebook (1999), http://www.fordham.edu/halsall/ancient/mesopotamia-contracts.html. (describing contracts for the sale of real estate, food, crops, and for rentals, leases, labor (employment), borrowing money, and so on).

A. An Overview of Blockchain Technology[2]

Blockchains are best conceptualized as a database maintained by a distributed network of computers. They blend together peer-to-peer networks, public-private key cryptography, and a set of rules—called a "consensus mechanism"—to manage how information is recorded in the shared database and verified by the network. By combining these technologies, blockchains can store tamper-resistant, resilient, and non-repudiable data in a transparent manner.[3]

Unlike today's databases, which are centrally maintained, no one single party controls a blockchain. Instead they are maintained by peer-to-peer networks. On widely supported blockchains, like Bitcoin and Ethereum, copies of the database are scattered across the globe, found on thousands of different computers at any given time.

Because blockchains are redundantly replicated, any data stored in a blockchain is widely available and resilient. If one individual version of a blockchain is corrupted, or if a member of a blockchain-based network stops participating, the event is of little significance. So long as one copy of a blockchain exists, other members of a network can access the information and continue to engage in transactions.

On a blockchain-based network, anyone can setup an "account," comprised of a public address (a public key) and a password (a private key). To engage in a transaction, a member of the network finds another user's public key and inputs their private key, thereby sealing the transaction with a "digital signature." Through this process, all transactions are authenticated and non-repudiable—the party that controls an account in a disputed transaction, will have a difficult time disputing that they did not engage in a transaction unless they can prove that their password (i.e., private key) was compromised.

Once executed, the transaction—along with other transactions—are grouped together into a block, which is then encrypted to form a number called a "hash." Each hash is unique to a block, and each block stores a reference to the previous block's hash, chaining the blocks together to form a sequential record of transactions on the network (hence why it is called a blockchain).

By linking blocks together, blockchains become tamper-resistant. A change to any record stored in a blockchain results in the generation of a new hash for a block, and thus changes the hash of every subsequent block in a blockchain, in effect, making the alteration readily apparent to those participating on the network.

To ensure that data is properly recorded to a blockchain and to further increase a blockchain's security, blockchain-based networks rely on a "consensus mechanism"— a set of rules that generally make it difficult to add information to a blockchain and even more difficult to tamper-with or change. There are several different types of consensus mechanisms, but the most popular one currently used today is a consensus mechanism commonly called "proof of work."

[2] For the purpose of this report, we limit our inquiry to public, permissionless blockchains. There are types of blockchains, which are private and permissioned. They are outside the scope of this report.

[3] Arvind Narayanan et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. (2016).

The proof of work consensus mechanism is a strict procedure for adding new blocks to the shared database and verifying that each block contains valid transactions and a valid hash. While generating a hash for any given block does not need to be a challenging task, blockchains relying on this type of consensus mechanism make this task difficult by requiring that a block's hash begin with a dynamically adjusted number of leading zeroes. Any computer trying to generate a valid hash must run repeated calculations through a brute force guessing game to meet the protocol's stringent requirements—a process often referred to as "mining"—forcing members of the network to dedicate computational resources and pay for hardware and electricity necessary to perform these computations. Blockchain-based networks adjust the difficulty of the guessing game, depending on the total computational power of the miners on the network, to ensure that the network adds a new block in predictable time intervals.[4]

Through this process, a blockchain's underlying protocol enables the network to reach consensus as to the state of the shared database periodically, while simultaneously preventing parties from creating fake transactions or otherwise altering the records stored in a blockchain. Because each block incorporates a hash of the preceding block, anyone trying to modify the content stored in a block will inevitably break the chain. And, for anyone to modify even a single record on a blockchain employing a proof of work consensus mechanism, a would-be attacker, or group of attackers, would have to go through the computationally expensive task of generating new hashes for every subsequent block in a blockchain at a pace that is faster than the majority of honest parties supporting the network, a task that have estimated costs in excess of $1 billion for the Bitcoin blockchain.[5]

B. Blockchain-Based Smart Contracts as Legal Contracts

Because blockchains store tamper resilient, transparent, and non-repudiable data, the technology is being used for far more than just maintaining records of digital currency transactions. Indeed, blockchains are storing or referencing, other forms of information; blockchain-based protocols are layering additional technology to process what can essentially be thought of as small computer programs—what technologists often refer to as "smart contracts." [6]

The first blockchain to enable the creation and deployment of sophisticated smart contracts was the Ethereum blockchain.[7] Announced in February of 2014, and launched roughly a year and a half later, Ethereum implements a blockchain and a decentralized computing platform (the Ethereum Virtual Machine), which processes a Turing-complete programming language. Using Ethereum, anyone can write, store, and execute small computer programs via a blockchain-based

[4] *Id.*

[5] Andrew Kim et al. The Stateless Currency and the State: An Examination of the Feasibility of a State Attack on Bitcoin (2014); Cost of a 51% Attack. https://gobitcoin.io/tools/cost-51-attack/ (estimating the cost of engaging in a 51% attack at over $1 billion dollars as of April 30, 2017).

[6] Vitalik Buterin. Ethereum Whitepaper. https://github.com/ethereum/wiki/wiki/White-Paper.

[7] Bitcoin features a non-Turing complete scripting language. Using this language smart contracts can be created but are limited to basic arithmetic, logic and cryptographic operations (e.g. hashing and verifying a signature). Massimo Bartoletti and Livio Pompianu. An Empirical Analysis of Smart Contracts: Platforms, Applications and Design Patterns (2017), https://arxiv.org/pdf/1703.06322.pdf .

network.[8] These computer programs are executed by multiple parties on the Ethereum network and thus have the capability to operate autonomously and independent of the control of any individual party.[9]

Smart contracts are being used to model and govern contractual relationships, structure a range of commercial arrangements from complex financial transactions—such as syndicated loans, options, and swaps—to royalty agreements involving copyrighted works.[10] Currently, the use of smart contracts in the context of legal arrangements, falls on a spectrum. On one end of the spectrum, for simple transactions, parties are relying entirely on smart contracts to model commercial relationships without the use of legal prose. A smart contract and its corresponding data are stored on a blockchain, where computer code governs entire commercial relationships, including payment obligations, asset transfers, and the terms and conditions of an arrangement.[11]

At the other end of the spectrum, smart contracts are being used to memorialize a portion of a parties' agreement, with a smart contract assisting with one or more performance obligations and traditional legal prose memorializing other basic contractual rights, obligations, and conditions—such as representations and warranties and choice of law and dispute resolution provisions. These "hybrid" agreements blend together traditional legal prose—written in a natural language like English—with smart contract programs written in code. The written agreement references and incorporates a smart contract and contextualizes how the program fits into a larger contractual arrangement.[12]

In many ways, legal agreements relying on smart contracts are no different than today's agreements. If parties choose to rely on a smart contract for purposes of a commercial relationship, they must first negotiate the terms of their agreement and ideally reach a "meeting of the minds."[13] Once an agreement is reached, parties reduce their understanding to a writing, choosing either to

[8] With Solidity, it is theoretically possible to execute a range of complex computations using a peer-to-peer network, creating software programs that are both hard to modify and potentially autonomous. Buterin, *supra* note 5. ("An important note is that the Ethereum virtual machine is Turing-complete; this means that EVM code can encode any computation that can be conceivably carried out, including infinite loops"); Wood, *supra* note 86; Hirai, Yoichi. "The Solidity Programming Language." The Ethereum Wiki. https://github.com/ethereum/wiki/wiki/The-Solidity-Programming-Language. Last edited Dec. 15, 2016.

[9] Buterin, *supra* note 6.

[10] John Ream et al., Upgrading Blockchains: Smart Contract Use Cases in Industry. Deloitte University Press, available at https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-based-smart-contract-use-cases-in-industry.html .

[11] *See, e.g.*, Ujo Music, Imogen Heap Alpha, https://alpha.ujomusic.com/#/imogen_heap/tiny_human/tiny_human.; OpenBazaar, https://openbazaar.org/; SafeMarket, https://safemarket.github.io/.

[12] Steven Norton. Law Firm Hogan Lovells Learns to Grapple with Blockchain Contracts. WSJ.com. February 2, 2017. http://blogs.wsj.com/cio/2017/02/01/law-firm-hogan-lovells-learns-to-grapple-with-blockchain-contracts/.

[13] Stephen J. Choi and Gulati Mitu. Contract as Statute. 104 Mich. L. Rev. 1129 (2006) (noting that "the traditional model of contract interpretation focuses on the "meeting of the minds.").

rely exclusively on a smart contract or draft a hybrid agreement.[14] In the case of a dispute, parties will either renegotiate the underlying arrangement or seek redress from a court or an arbitration panel to revert the effects of a smart contract.[15]

Where traditional legal agreements and agreements relying on smart contracts differ is how smart contracts handle performance obligations. With contracts that only rely on natural language provisions, each party to the contract is responsible for performing contractual obligations and can choose to halt their performance at any time (and, if necessary, face the legal consequences of a breach).

In arrangements relying on smart contracts, performance obligations are memorialized in code using a strict and formal programming language and executed by members of a blockchain-based network. For example, using Ethereum, each smart contract is assigned a blockchain-based address. The code of the smart contract is stored on each miner's computer. Parties initiate a smart contract by sending digitally signed "transactions" to the smart contract's address. The "transaction" is a record which includes, amongst other things, the variables necessary for the smart contract code to run, along with a digital signature of the sending party. The transactional record is stored on the Ethereum blockchain. Once stored, the saved record triggers the smart contract's execution and the smart contract's code is run by all miners supporting the network.

In effect, once a smart contract is triggered via a transaction by one of the parties, the smart contract acts as the parties' agent, deputized to assist the parties with their arrangement. However, unlike traditional agents, smart contracts operate autonomously by default. Multiple parties on a blockchain-based network execute the smart contract code by virtue of its distributed nature, thus parties relying on the smart contract lack the ability to halt the smart contract's execution unless provided for in the underlying code.

By implication, performance obligations memorialized in a smart contract can be designed to be difficult to terminate. Parties can rely on a blockchain network, to gain a high degree of assurance that any contractual obligations memorialized using a smart contract will be performed.[16] By relying on code that is potentially autonomous, and thus difficult to terminate or change, parties can reduce their need to monitor performance obligations on an ongoing basis, at least as compared to obligations memorialized with a traditional contract.

[14] It is important to emphasize that not all contractual agreements operate in this manner. As Ian Macneil has noted, many contracts are not discrete and pre-negotiated, but evolve from an ongoing relationship between the parties. This so called "relational contracting" differs because typically there is no single moment at which the parties confirm a meeting of the minds. The contracting process is gradual, as parties gather more information about the other. *See* Ian R Macneil. The New Social Contract: An Inquiry Into Modern Contractual Relations. (1980); *see also* Ian R. Macneil. Contracts: Adjustment of Long-Term Economic Relations under Classical, Neoclassical, and Relational Contract Law. 71 Nw. UL Rev. 854 (1977).

[15] Of course, even if it is always possible to go through the traditional legal systems to seek redress, the effects of a smart contracts could, in some situations, be difficult to revert in full. For instance, in cases where the parties' funds are stuck into an automated escrow.

[16] Filippi, Primavera De, and Aaron Wright. *Blockchain and the Law the Rule of Code*. Harvard University Press, 174 (2018).

Moreover, because smart contracts are written in computer code, they can be designed to be more dynamic than traditional legal prose and can be constructed to adjust performance obligations during the term of an agreement using a trusted third-party source—commonly referred to by programmers as *oracles*.[17] Oracles can be individuals or programs that store and transmit information from the outside world, thereby providing a means for blockchain-based systems to interact with real-world persons and potentially react to external events. Oracles can be connected, for example, to a data feed from a third party conveying the latest London Interbank Offered Rate (LIBOR), or they can be sensors that transmit temperature, humidity, or other relevant information about a location. More experimental, an oracle can also be made to convey the insights of human beings or support private dispute resolution and private arbitration systems (sometimes referred to as judge-as-a-Service or arbitration-as-a-Service).[18]

Using oracles, smart contracts can respond to changing conditions in near real time. [19] Parties to a contract can reference an oracle to modify payment flows or alter encoded rights and obligations according to new information. Oracles also make it possible to determine or update specific performance obligations based on the subjective and arbitrary judgment of individuals. In this way, parties can rely on the deterministic and guaranteed execution of smart contracts for objective promises that are readily translatable into code. At the same time, they can assign to a human-based oracle the task of assessing promises that cannot easily be encoded into a smart contract, either because they are too ambiguous or because they require a subjective assessment of real world events.[20]

By virtue of the fact that smart contracts are written in code, smart contracts also have the potential to be more precise and could be bundled over time to form modular software libraries that improve the efficiency of creating and executing legal agreements. Indeed, smart contracts can even be tested before execution to ward off potential mishaps in the code and to confirm the intent of each party.[21]

For example, consider the below smart contract, which facilitates a simple auction on the Ethereum blockchain. Here, a party auctioning off an item can publicly identify an item for sale and find interested parties. Those that are interested can rely on the smart contract to manage the sale of the item, gaining assurance that the auction process will not be rigged by the party setting up the sale.

[17] Alec Liu. Smart Oracles: Building Business Logic With Smart Contracts. Ripple. July 16, 2014. https://ripple.com/insights/smart-oracles-building-business-logic-with-smart-contracts/; Vitalik Buterin. Ethereum and Oracles. Ethereum Blog. July 22, 2014. https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/.

[18] Michael del Castillo. Lawyers Be DAMNed: Andreas Antonopoulos Takes Aim at Arbitration With DAO Proposal. CoinDesk. May, 26, 2016. http://www.coindesk.com/damned-dao-andreas-antonopoulos-third-key/.

[19] Ethan M. Katsh. Law in a Digital World (1995).

[20] Pietro Ortolani, Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin. 36 Oxford J. Legal Studies 595 (2015).

[21] *See* Mintchalk, http://www.mintchalk.com. For example, a smart contract has been created which simulates the mechanics of a crowd funding campaign in 56 lines of code. See id. at http://www.mintchalk.com/c/68f3e.

The code follows a strict logic whereby parties interested in bidding can send a bid denominated in Ethereum's native token "ether" by executing a transaction on the Ethereum network. The smart contract keeps track of the highest bid. Once the auction ends, the party setting up the auction can collect ether by simply sending their own signed transaction to the smart contract.[22] Once the transaction is sent, the account of the "winning" party is debited.

```
pragma solidity ^0.4.11;

contract SimpleAuction {
    address public beneficiary;
    uint public auctionStart;
    uint public biddingTime;

    address public highestBidder;
    uint public highestBid;

    mapping(address => uint) pendingReturns;

    bool ended;

    event HighestBidIncreased(address bidder, uint amount);
    event AuctionEnded(address winner, uint amount);

    function SimpleAuction(
        uint _biddingTime,
        address _beneficiary
    ) {
        beneficiary = _beneficiary;
        auctionStart = now;
        biddingTime = _biddingTime;
    }

    function bid() payable {
        require(now <= (auctionStart + biddingTime));
        require(msg.value > highestBid);
        if (highestBidder != 0) {
            pendingReturns[highestBidder] += highestBid;
        }
        highestBidder = msg.sender;
        highestBid = msg.value;
        HighestBidIncreased(msg.sender, msg.value);
    }
    function withdraw() returns (bool) {
        var amount = pendingReturns[msg.sender];
        if (amount > 0) {
```

[22] Simple Open Auction, http://solidity.readthedocs.io/en/develop/solidity-by-example.html.

```
         pendingReturns[msg.sender] = 0;
         if (!msg.sender.send(amount)) {
            // No need to call throw here, just reset the amount owing
            pendingReturns[msg.sender] = amount;
            return false;
         }
      }
      return true;
   }
   function auctionEnd() {
      require(now >= (auctionStart + biddingTime));
      require(!ended);
      ended = true;
      AuctionEnded(highestBidder, highestBid);
      beneficiary.transfer(highestBid);
   }
}
```

Figure 1: Example Smart Contract

Even though the mechanics of the auction follows the strict logic of the code, this smart contract—as well as other smart contracts more generally—have limitations and drawbacks. First, if the smart contract contains a mistake, security flaw, or does not accurately capture the parties' intent, the smart contracts will be difficult to modify or change, due to a blockchain's resilient and tamper-resistant nature. If someone mistakenly overbids for an item, there will be no central party to petition to reverse the transaction. The program will continue to blindly execute its code, regardless of the intent of the parties or changed circumstances.

Second, the smart contract does not entirely remove the need for trust and coordination between parties. For instance, in the above example, bidders still need to affirmatively send bids to the smart contract by signing blockchain-based transactions. And if the auction involves the sale of a physical good, the parties bidding still need to trust that the party auctioning off the good will deliver the product as promised. The smart contract does not create a purely automated transaction. It merely automates a narrow set of payment obligations.

Third, smart contacts and blockchain technology exhibit certain security vulnerabilities, which could temper the desire of parties to onboard high-value commercial transactions. Blockchains are vulnerable to certain attacks which, if effectuated, could result in a blockchain splitting into two separately maintained databases (through a process called "forking").[23] In the event of a fork, a mal-intentioned actor could invalidate certain smart contract transactions or attempt to improperly transfer digital currency or other digital assets represented on a blockchain. The code of a smart contract is also susceptible to security vulnerabilities and exploits, which could

[23] Castor, Amy. A Short Guide to Bitcoin Forks, http://www.coindesk.com/short-guide-bitcoin-forks-explained/.

cause a smart contract to operate unexpectedly, or worse, enable a third-party to siphon digital currency or other assets from contracting parties accounts.[24]

II. Legal Enforceability of a Smart Contract

Even though the use of smart contracts in the context of legal arrangements may provide parties with certain advantages, the use of this code will not operate in a legal vacuum. Deployment of smart contracts in commercial settings will inevitably lead to disputes. For example, if smart contract code is flawed, incorporates a poorly drafted provision, or executes in a manner not intended by one of the parties, parties will likely turn to the legal system to resolve the contractual dispute, thus an analysis of whether or not smart contracts can form a legally binding agreement is required.

Given the novelty of the technology, the question of the enforceability of smart contract code has not yet been examined by U.S. courts. Fortunately, the question of smart contract enforceability can be largely answered under existing state law implementations of the statute of frauds, the Uniform Commercial Code ("U.C.C."), the Electronic Signatures in Global and National Commerce Act ("E-Sign Act"), and state laws modeled on the Uniform Electronic Transactions Act ("UETA").

A. The Statute of Frauds

At its most generalized level, a contract is nothing more than a "promise or 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."[25] For a contract to be binding, there must be competent parties, sufficiently definite terms, mutual assent and performance, and an exchange of value or another form of consideration.[26]

Even though contracts may be oral or implied, every state in the U.S., except Louisiana, has adopted one or more statutes, known collectively as the "statute of frauds," which identify agreements that are enforceable only if they are in writing and signed.[27] Moreover, the U.C.C. also imposes writing requirements for: (i) contracts for the sale of goods priced $500 or more; (ii)

[24] For example: After the Distributed Autonomous Organization (DAO) hack, the Ethereum blockchain forked into Ethereum and Ethereum Classic. Alyssa Hertig. Ethereum's Two Ethereums Explained, http://www.coindesk.com/ethereum-classic-explained-blockchain/.

[25] Restatement (Second) of Contracts § 1.

[26] *Id.* § 16 (intoxication); *id.* §18 (both parties have made promise or started performance); *id.* § 20 (mutual assent); *id.* § 33 (definite terms); *id.* § 71 (consideration). Promises might be enforceable when there is no consideration through promissory estoppel or the material benefit rule. *Id.* §§ 86, 90.

[27] Louisiana does not have a statute of frauds, but it does have writing requirements. Louisiana Code Article 2275 and 2462 require that contracts related to immovable property be in writing. Leases are exempted. Article 2241 requires that the parties both sign the document. Article 2278 requires a writing for promises to pay a third person's debt. Additional writing requirements exist beyond the discussed articles, scattered through the Louisiana laws. M. Thomas Arceneux, Writing Requirements and the Authentic Act in Louisiana Law: Civil Code Articles 2236, 2275, & 2278. 35 Louisiana L. Rev. 764 (1975).

agreements that create a security interest in personal property if the property is not in the secured party's possession, a certificated security, or collateral that consists of deposit accounts, investment property, letter-of-credit rights, or electronic chattel paper if the secured party has control over such collateral; and (iii) lease agreements requiring total payments of more than $1,000.[1] These statutes define the boundaries of contract enforceability and require that certain agreements be in writing "to protect . . . parties and preserve the integrity of contractual agreements," guarding "against the peril of perjury" and "prevent[ing] the enforcement of unfounded fraudulent claims."[28]

1. Overview of the Statute of Frauds and U.C.C. Writing Requirements

The statute of frauds generally requires that certain types of agreements be memorialized in writing: (i) agreements relating to executorship, suretyship, marriage[29], and performance over one year; (ii) agreements for the transfer of an interest in land[30]; and (iii) agreements for the sale of goods over $500.[31]

Even if certain promises are memorialized in writing, the writing will not be deemed a valid contract under the statute of frauds if the writing—or series of writings—do not reasonably identify the contracting parties, fail to outline the subject matter of the contract and its essential terms, and fail to contain valid signatures from the parties or their agents.[32]

What qualifies as a valid writing under the statute of frauds is understandably flexible. A writing does not need to be thorough or complete.[33] The core requirement is that the writing contain the "material elements" of an agreement.[34] A writing can be memorialized in an electronic format and several writings may form an agreement, provided that they may be taken together to

[28] William J. Jenack Estate Appraisers & Auctioneers, Inc. v. Rabizadeh, 5 N.E.3d 976, 981 (2013).

[29] Agreements and promises made in consideration of marriage must be evidenced by a writing to be enforceable. N.Y. Gen. Oblig. § 5-701; Del. Code Ann. tit. 6 § 2714.

[30] However, "where there is a verbal agreement under which each of the parties is to convey land to the other, it is generally held that a conveyance by one on the faith of the agreement constitutes such part performance as will in equity take the case out of the operation of the statute of frauds." In re Destro, 675 F.2d 1037, 1038 (9th Cir. 1982).

[31] Restatement (Second) Contracts § 110; N.Y. Gen. Oblig. § 5-701; Del. Code Ann. tit. 6 § 2714. Note these agreements could be enforceable even if they do not meet the requirements of the statute of frauds if for example, there is evidence or reliance or an implied contract. Restatement (Second) of Contracts § 139.

[32] Restatement (Second) Contracts § 131 (1981); N.Y. Gen. Oblig. § 5-701; Del. Code Ann. tit. 6 § 2714.

[33] Lamle v. Mattel, Inc., 394 F.3d 1355, 1361 (Fed. Cir. 2005) ("we conclude that under California law the . . . email satisfies the Statute of Frauds.); Levin v. Knight, 780 F.2d 786, 787 (9th Cir. 1986)

[34] Willmott v. Giarraputo, 157 N.E.2d 282, 282 (N.Y. 1959); Brown v. Cara, 420 F.3d 148, 150 (2d Cir. 2005); Huntington Towers, Ltd. v. Franklin Nat'l Bank, 559 F.2d 863, 864 (2d Cir. 1977); Canister Co. v. Wood & Selick, Inc., 73 F.2d 312, 315 (3d Cir. 1934); Conner v. Lavaca Hosp. Dist., 267 F.3d 426, 430 (5th Cir. 2001).

provide evidence of the validity of a contract.[35] Importantly, a writing does not need to be entirely written in legal prose. A writing can reference data and contain formulas.[36]

The test for what qualifies as "essential terms" is open-ended and transaction specific. [37] Courts generally characterize "essential terms" as those terms which are "customarily encountered" for a given transaction, including terms such as a purchase price, subject matter of the agreement, the time and term of payment, closing dates, and information sufficient to identify any conveyed title.[38]

Likewise, there are no formal requirements related to what does and does not qualify as permissible signatures.[39] A valid signature can be any symbol that a party makes with the intent to authenticate a record or contract,[40] including a traditional ink signature, initials, a typed or printed signature, a signature created with a rubber stamp, and can be located at any part of a document.[41]

When evaluating whether an agreement satisfies the statute of frauds, courts have long deployed common sense and commercial experience in assessing whether a writing is valid and creates an enforceable contract. In making such determinations, courts generally place weight on the intent of the parties and whether the signing party executed or adopted the signature with an intention to authenticate the writing.[42]

For example, over a century ago, the United States Supreme Court in *Bibb v. Allen*, 149 U.S. 481 (1893), grappled with the question of whether to enforce an electronically communicated and created agreement, finding a valid agreement involving a futures contract for cotton transmitted over a telegraph.[43] There, the Court found a valid agreement, because the parties "agree[d] upon the terms in which the business should be transacted," and intended to be bound.[44]

[35] Crabtree v. Elizabeth Arden Sales Corp., 110 N.E.2d 551, 552 (N.Y. 1953); Affiliated Invest., Inc. v. Turner, 337 So. 2d 1263, 1264 (Miss. 1976); QUINN-SHEPHERDSON CO. v. TRIUMPH FARMERS ELEVATOR CO., 182 N.W. 710, 710 (Minn. 1921); Johnson & Miller v. Buck, 35 N.J.L. 338, 340 (1872); Casazza v. Kiser, 313 F.3d 414, 419 (8th Cir. 2002).

[36] United States v. Bethlehem Steel Corp., 62 S. Ct. 581 (1942); Tractebel Energy Mktg. v. AEP Power Mktg., 487 F.3d 89 (2d Cir. 2007); Doyle v. Wohlrabe, 66 N.W.2d 757, 762 (Minn. 1954).

[37] Lamle, 394 F.3d at 1361 (What is an essential term "depends on the agreement and its context and also on the subsequent conduct of the parties.").

[38] Nesbitt v. Penalver, 835 N.Y.S.2d 426, 429 (2d Dep't 2007); Levin v. Knight, 780 F.2d 786, 787 (9th Cir. 1986) (the Ninth Circuit, interpreting California law, has stated that "the subject matter, the price, and the party against whom enforcement is sought" are the "few terms deemed essential as a matter of law by California courts."); Wilcher v. City of Wilmington, 139 F.3d 366, 373 (3d Cir. 1998) ("Until it is reasonable to conclude . . . that all of the points that the parties themselves regard as essential have been expressly or . . . implicitly resolved, the parties have not … formed a contract.");

[39] U.C.C. § 1-201 cmt 37.

[40] Restatement (Second) Contracts § 134; U.C.C. § 1-201(39).

[41] *Id.* § 134; Flight Sys. v. Electronic Data Sys. Corp., 112 F.3d 124, 129 (3d Cir 1997); Hessenthaler v. Farzin, 564 A.2d 990 (Sup. Ct. Pa. 1989).

[42] U.C.C. § 1-201 cmt 37.

[43] Bibb v. Allen, 149 U.S. 481 (1893).

[44] *Id.*

The fact that key terms of the relevant agreement were memorialized using The Shepperson Cotton Code, a popular encrypted telegraphic code at the turn of the twentieth century used for the cotton trade made little difference, because the parties contemplated using the code to engage in commercial activity.

At the same time, however, courts have voided agreements where signatures were deemed to be automatic and not indicative of a parties' intent. By way of illustration, in *Parma Tile Mosaic & Marble Co., Inc. v. Estate of Shor*t, 87 N.Y.2d 524 (N.Y. 1996), the New York Court of Appeals held that an automatic fax machine heading printed on a document did not satisfy the statute of frauds signature requirement. The court held that under the statute of frauds, a valid signature requires an intentional act to authenticate the writing. Where the name or signature is automatically generated without regard to the underlying document, the statute of frauds is not satisfied and the contract is not enforceable.[45]

Agreements covered by the U.C.C. have comparable, but slightly different writing requirements. For contracts over $500 involving the sale of goods, the writing must indicate, at a minimum, that a contract for sale has been made between the parties and reasonably identify the subject matter of the agreement.[46] The writing must also show the price as a "defined or stated price."[47] If there is no writing, an agreement will still be enforceable if "payment has been made and accepted" by the purchasing party.[48]

For contracts involving lease agreements with total payments over $1,000, the writing must sufficiently indicate that a lease contract has been made and detail the total payments under the lease, the lease term, and describe the goods leased.[49] Like with the sale of goods over $500, a lease will still be deemed enforceable with respect to goods that have been received and accepted by the lessee.[50]

[45] 87 N.Y.2d 524 (N.Y. 1996).

[46] U.C.C. § 1-206.

[47] *Id.* § 2-201. A contract for the sale of goods will also be valid, even if it is not in writing, if: (i) "the goods are to be specially manufactured for the buyer and are not suitable for sale to others in the ordinary course of the seller's business and the seller, before notice of repudiation is received and under circumstances which reasonably indicate that the goods are for the buyer, has made either a substantial beginning of their manufacture or commitments for their procurement"; or (ii) "the party against whom enforcement is sought admits in his pleading, testimony or otherwise in court that a contract for sale was made, but the contract is not enforceable under this provision beyond the quantity of goods admitted." *Id.*

[48] *Id.* § 2A-201. A lease agreement also will be valid, even if it is not in writing if: (i) "if the goods are to be specially manufactured or obtained for the lessee and are not suitable for lease or sale to others in the ordinary course of the lessor's business, and the lessor, before notice of repudiation is received and under circumstances that reasonably indicate that the goods are for the lessee, has made either a substantial beginning of their manufacture or commitments for their procurement"; or "the party against whom enforcement is sought admits in that party's pleading, testimony or otherwise in court that a lease contract was made, but the lease contract is not enforceable under this provision beyond the quantity of goods admitted. *Id.*

[49] *Id.* § 2A-201.

[50] *Id.*

Contracts that only involve a security interest will be "enforceable against the debtor and third parties with respect to collateral if the debtor has authenticated a security agreement that provides a description of the collateral and, if the security interest covers timber to be cut, a description of the land concerned"[51] In general, contracts for the "sale or purchase of a security [are] enforceable whether or not there is a writing signed or record authenticated," so long as "value has been given" and the debtor has "rights in the collateral."[52]

The U.C.C. also has flexible signature requirements. Both contracts for the sale of goods and lease agreements require that the writing be signed, "using any symbol executed or adopted with present intention to adopt or accept a writing."[53] The U.C.C. does not provide a "catalog of possible [signing] situation[s],"[54] leaving it to courts to apply "common sense and commercial experience" to determine whether "the symbol was executed or adopted by the party with present intention to adopt or accept the writing."[55] Contracts involving a security interest, simply require that the relevant writing be "authenticated" by "signing" the document "with present intent to adopt or accept a record, to attach to or logically associate with the record an electronic sound, symbol or process."[56]

2. Use of Smart Contracts in Legal Agreements under the Statute of Frauds

The use of smart contracts to govern a contractual arrangement should satisfy the statute of frauds. To create an enforceable agreement, contracting parties must manifest an intent to be bound and satisfy basic requirements for contract formation, including reasonably identifying the parties and outlining material terms of an arrangement. The agreement must be accompanied by valid signatures which are not automatically generated.

Accordingly, the code of a smart contract and any data stored in a transaction used to trigger a smart contract can—in certain instances—represent the essential terms and conditions of an agreement.[57] A smart contract can be written to facilitate payment—including at set time-periods—and can transfer title to property represented on a blockchain. Parties seeking to use a smart contract can enter into a transaction that initiates the smart contract code's execution, and the record related to the transaction can contain relevant information about a parties' agreement. Thus, the initiating transaction and the smart contract code, when viewed together, can memorialize the material terms of certain agreements.[58]

[51] *Id.* § 9-203(b)(3)(A). If the "collateral is not a certificated security and is in possession of the secured party" or "the collateral is a certificated security in registered form and the security certificate has been delivered to the secured party," or "the collateral is deposit accounts, electronic chattel paper, investment property, letter-of-credit right, or electronic documents and the secured party has control" then it is unnecessary for the debtor to "authenticat[e] [the] security agreement." *Id.* § 9-2039(b).

[52] *Id.* § 8-113(a); An exception to inapplicability of the statute of frauds to securities exists for "contracts for the sale or purchase of a cooperative interest." *Id.* § 8-113(b)

[53] *Id.* § 1-201(37).

[54] *Id.*§ 1-201 cmt. 37.

[55] *Id.*

[56] *Id.* § 9-102(7).

[57] Restatement (Second) Contracts § 131 (1981); N.Y. Gen. Oblig. § 5-701; Del. Code Ann. tit. 6 § 2714.

[58] For example, the subject matter of the agreement could be delineated in the comments of the smart contract code.

Indeed, even if a smart contract relies on outside data feeds or oracles, the above analysis should not change. Courts have routinely held that formulas—even indefinite ones—can be sufficient for fulfilling the price terms of contracts so long as the parties agree to rely on the formula and agree to reference an outside data source.[59]

Blockchain-based transactional records and the digital signatures associated with these records should also satisfy the statute of fraud's writing requirements. As noted above, the test for what qualifies as a valid signature is flexible and can include "[a]ny mark affixed to a writing with the intent to authenticate" the contract.[60] Typewritten signatures and electronic records stored by computing devices have been found sufficient to satisfy the requirements of the statute of frauds. Thus transactional records and associated digital signatures stored in a blockchain should also be deemed sufficient to satisfy the statute of frauds.

For instance in *Lamle v. Mattel*, 394 F.3d 1355 (Fed. Cir. 2005), the Federal Circuit determined that an email and an accompanying typewritten name could satisfy the statute of frauds, because courts have held that "typed names appearing on the end of telegrams are sufficient to be writings under the Statute of Frauds" because there is "no meaningful difference between a typewritten signature on a telegram and an email."[61]

For much the same reason, there is no meaningful difference between a typewritten name and a digital signature affixed to a transaction triggering a smart contract using public private key cryptography, assuming the address can be uniquely tied to the signing party. The purpose of the "statute of frauds is to prevent a contracting party from creating a triable issue concerning the terms of the contract—or for that matter concerning whether a contract even exists—on the basis" of one party's word.[62] It is for that reason that neither the common law nor the U.C.C. requires a handwritten signature.[63]

Similar reasoning should apply to public-private key cryptography where there is verifiable evidence "and not merely say-so evidence" establishing an intent by a party to be bound to a contractual arrangement.[64] A digital signature associated with a blockchain-based transaction requires a volitional act on the part of the signing party—the inputting of a private key—and thus should satisfy the statute of frauds.

[59] Citadel Grp. v. Wash. Reg'l Med. Ctr., 692 F.3d 580, 582 (7th Cir. 2012); Arbitron, Inc. v. Tralyn Broad., Inc., 400 F.3d 130, 136 (2d Cir. 2005); Piven v. Wolf Haldenstein Adler Freeman & Herz L.L.P., 2010 WL 1257326, at *12 (S.D.N.Y. Mar. 12, 2010); Cobble Hill Nursing Home, Inc. v. Henry & Warren Corp., 74 N.Y.2d 475, 483 (1989).

[60] 4 Williston, Contracts § 585 (3rd ed. 1961).

[61] 394 F.3d at 1362; *see also* Mirchel v. RMJ Sec. Corp., 613 N.Y.S.2d 876, 878 (1st Dep't 1994) ("documentary evidence in defendant's own files . . . and defendant's computer records . . . satisfy any writing requirement under the Statute of Frauds.").

[62] Cloud Corp. v. Hasbro, Inc., 314 F.3d 289, 296 (7th Cir. 2002).

[63] *Id.*; Just Pants v. Wagner, 617 N.E.2d 246, 251 (Ill. App. Ct. 1993); Monetti, S.P.A. v. Anchor Hocking Corp., supra, 931 F.2d 1178, 1182 (7th Cir. 1991); Hillstrom v. Gosnay, 614 P.2d 466, 469 (Mont. 1980); 810 Ill. Comp. Stat. Ann. 5/1-201 cmt. 37; Restatement (Second) of Contracts § 134, cmt. a (1981).

[64] Cloud Corp., 313 F.3d at 296; *see also* Consolidation Services, Inc. v. KeyBank National Ass'n, 185 F.3d 817, 821 (7th Cir.1999); Monetti, S.P.A., 931 F.2d at 1183.

If a smart contract is incorporated by reference into a standard legal agreement, the risk that the agreement would fail to satisfy the statute of frauds lessens. Such an agreement could readily satisfy the statute of frauds writing requirement and could outline the material terms of a parties' arrangement. Signatures could be typewritten, or signed by hand, and the smart contract code could be made a material part of the arrangement.

Indeed, contracting parties have long relied on comparable "hybrid" agreements in arrangements involving the exchange of other electronic information. Since the late 1970s, contracting parties—particularly large corporations—have relied on electronic data interchange ("EDI") systems to swap electronic purchase orders, invoices, bills of lading, inventory data, and various types of confirmations to manage their ongoing commercial relationships, eliminating paperwork and reducing labor and transaction costs."[65]

With EDI arrangements, parties often execute master agreements that contextualize the use of electronic messaging in the context of a broader contractual relationship.[66] They sign traditional paper agreements governing the exchange of messages between themselves and rely on EDI systems to manage an ongoing trading partnership.[67]

These master agreements generally confirm, *inter alia*, that the parties will "electronically transmit to or receive from the other party any of the transactions" via EDI systems. The parties further: (i) affirm their "mutual intent . . .to create binding purchase and sale obligations pursuant to . . . electronic transmission[s]"; (ii) acknowledge that electronic messages and transmissions will be considered a "writing" or "in writing"; and (iii) establish that the use of electronic messages will "evidence a course of dealing and course of performance accepted by the parties." To further gird against an enforceability challenge, parties warrant "not to contest the enforceability" of the agreement.[68]

A similar structure could be adopted for arrangements involving smart contracts. A master agreement could address potential enforceability issues raised by a smart contract and provided additional context as to the subject matter and intent of the parties should a dispute arise in the future. Parties could confirm that a smart contract is being used to govern key performance obligations and the master agreement could outline terms, conditions, and other contractual provisions that will not be readily translatable into code—provisions such as representations and warranties, dispute resolution provisions, and other standard boilerplate clauses.

3. Use of Smart Contracts for Legal Agreements Covered by U.C.C. Statute of Frauds Requirements.

[65] Wittie, Robert A., and Jane K. Winn. Electronic Records and Signatures under the Federal E-SIGN Legislation and the UETA. 55 The Business Lawyer 293 (2000).

[66] *Id.*

[67] *Id.*

[68] The Electronic Messaging Services Task Force, The Commercial Use of Electronic Data Interchange-A Report and Model Trading Partner Agreement, 45 Bus. Law. 1645, 1746 (1990).

A smart contract—in and of itself—can also create an enforceable agreement involving the sale of goods over $500. Under Article 2 of the U.C.C., a contract for the sale of goods will only be deemed enforceable if: (i) there is a writing that indicates that a contract for sale has been made; and (ii) the writing is signed by the party against whom enforcement of the contract is sought.[69]

A smart contract and the blockchain-based transaction triggering the smart contract should both qualify as valid "writings." Under the U.C.C, a "writing" is broadly defined to cover any "printing, typewriting or any other intentional reduction to tangible form,"[70] and electronic records, like e-mail, have been found to satisfy the U.C.C.'s writing requirements. Because a smart contract and the related transactional information can be fairly construed as electronic records, a smart contracts and the blockchain-based transactions triggering the smart contracts should both should satisfy the U.C.C.'s writing requirements.[71]

A digital signature related to a blockchain-based transaction should also qualify as a valid signature. As noted above, the U.C.C. does not define the manner in which a signature needs to be represented, and courts analyze whether there is a valid signature by assessing whether there is evidence that the parties "adopted or accepted" the writing. [72] A seller or purchaser of a good relying on a smart contract could effectively indicate their assent to an agreement when they input their private key to send the blockchain-based transaction.

Data stored in a transactional record used to initiate a smart contract—when viewed in conjunction with a smart contract's code—can further indicate that a contract for sale has been made. The transactional record can contain relevant payment terms and include a reference to a good which is represented or tracked on a blockchain—i.e., the relevant good could be "tokenized." [73]

Smart contracts concerning leases over $1,000 can also be constructed to comply with the requirements of the U.C.C. Unless an exception applies, to meet Article 2A's statute of frauds, a writing concerning a lease must detail the total payments under the lease, the lease term, and describe the goods leased.[74] An exact or precise description of the leased goods or the term of the lease is not required. All that is necessary is that the writing "reasonably identifies" the agreement's subject matter.[75]

[69] U.C.C. § 2-201.
[70] *Id.* § 1-201(43).
[71] Bazak Int'l Corp. v. Tarrant Apparel Grp., 378 F. Supp. 2d 377, 392 (S.D.N.Y. 2005); *see also* International Casings Group, Inc. v. Premium Standard Farms, Inc., 358 F. Supp. 2d 863, 872-875 (W.D. Mo. 2005); Roger Edwards, LLC v. Fiddes & Son, LTD, 245 F. Supp. 2d 251, 257-261 (D. Me. 2003); Central Illinois Light Company v. Consolidated Coal Company, 235 F. Supp. 2d 916, 919 (C.D. Ill. 2002); Commonwealth Aluminum Corporation v. Stanley Metal Associates, 186 F. Supp. 2d 770, 772-774 (W.D. Ky. 2001).
[72] *Id.*
[73] For more information about "tokens," *see* Linda Xie. "A Beginners Guide to Ethereum Tokens." The Coinbase Blog. May 22, 2017. https://blog.coinbase.com/a-beginners-guide-to-ethereum-tokens-fbd5611fe30b.
[74] U.C.C. § 2A-201.
[75] Anderson U.C.C. § 2A-201:33 (3d. ed.)

As with the sale of goods, a tokenized reference to property could be stored in a transactional record used to trigger a smart contract's code, along with the relevant term and payment obligations. The key provisions of a lease could thus be discerned by viewing the triggering transaction and the smart contract code.

However, a smart contact may not be able to fully satisfy U.C.C. writing requirements for transactions that create a security interest in personal property. While any property subject to a security interest could theoretically be represented on a blockchain—thereby describing relevant collateral—a smart contract could theoretically fail to contain a clear statement that a debtor is providing a security interest in relevant goods.

To address these limitations, and to limit any of the risks of non-enforceability under the U.C.C., contracting parties could craft a "hybrid agreement" that incorporate any necessary language found in a standard security agreement. As with the hybrid agreement described above, an agreement written in legal prose could contain representations and warranties, debtor covenants, and other assurances, and incorporate by reference a smart contract to handle lending and re-payment terms.

B. The ESIGN Act, UETA, and Related State Statutes

Further reducing the opportunity to challenge the enforceability of a legal agreement relying all or in part on smart contracts are the E-Sign Act, UETA, and similar state law variations. Generally, these acts—when applicable—establish that signatures, contracts, and other records cannot be denied legal effect solely because they are in electronic form.

1. Requirements of the UETA

Since 1999, 47 states, the District of Columbia, Puerto Rico, and the Virgin Islands have adopted the UETA. The UETA gives electronic records and electronic signatures the same legal effect as traditional, written documents and signatures in certain transactions. So long as each party to a contract has agreed to conduct the transaction electronically, under Section 7 of the UETA, an electronic record and electronic signature may not be denied legal effect or deemed unenforceable simply because either was in electronic form.[76] If a law requires a record to be in writing, or requires a signature, electronic versions will be deemed sufficient.[77]

The definitions in the UETA are broad and cover a range of electronic signatures and records. An "electronic record" includes any "record created, generated, sent, communicated, received, or stored by electronic means,"[78] including any "[i]nformation processing systems, computer equipment and programs" as well as any "information stored on a computer hard drive."[79] An "electronic signature" comprises any "electronic sound, symbol, or process attached

[76] UETA § 7(a), (c)-(d).

[77] *Id.* § 7 (c).

[78] *Id.* § 2 (7).

[79] *Id.* § 2, cmt. 6.

to or logically associated with a record and executed or adopted by a person with the intent to sign the record,"[80] and covers any "digital signature using public key encryption technology."[81]

As with traditional written signatures, when determining if an electronic signature creates an enforceable contract, courts assess whether the signer executed or adopted the signature with the intent to sign the record. The signature must be accompanied by an "intent to do a legally significant act."[82]

Importantly, UETA contemplates the use of computer programs—what the UETA terms an "electronic agent"—and other automated means of entering into binding agreements, stipulating that an agreement will not be denied legal effect simply because parties chose to use an "electronic agent" when engaging in commercial activity.

Under the UETA, an "electronic agent" broadly includes any "computer program" and other "automated means used to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual."[83] Electronic agents can "initiat[e], respond[e] or interact with other parties or their electronic agents" and may be "created with the ability to act autonomously, and not just automatically."[84] Contracts facilitated by electronic agents may be formed "even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements" and even contemplates "anonymous click-transactions," where a party engages in a transaction without providing identification.[85]

Despite the UETA's expansive nature, there are certain transactions specifically excluded from UETA. These state statutes only apply to "transactions related to business, commercial (including consumer) and governmental matters" and thus do not apply to transactions governed by: (i) laws relating to the creation and execution of wills, codicils, or testamentary trusts; (ii) contracts governed by the UCC, other than sections covering: (A) the waiver or renunciation of a claim or right after a breach of contract; (B) the sale of goods; (C) leases; or (D) any other specific law identified as exempt in a state's adopted version of the UETA.[86]

These exceptions are narrow. The UETA covers, *in toto*, transactions under U.C.C. Article 2 and 2A, as well as trusts in commercial and business settings.[87] If desired by the parties, the UETA even applies transactions involving real estate,[88] in an attempt to break down "existing

[80] *Id.* § 1.
[81] *Id.* § 1, cmt. 7.
[82] *Id.* § 2, cmt. 7.
[83] *Id.*
[84] *Id.* § 2, cmt. 5.
[85] *Id.* § 12, cmt 2.
[86] *Id.* § 3, cmt 1. UCC § 1-306, former section 1-107; UCC § 1-306, former section 1-107; UCC §§ 2A-101-2A-532; UETA § 3(b). The UETA also does not apply to transactions governed by the Uniform Computer Information Transactions Act, which has only been adopted in Maryland and Virginia. Md. Code Ann., Com. Law § 22. Maryland Uniform Computer Information Transactions Act; Va. Code Ann. § 59.1, Chpt. 43. Uniform Computer Information Transactions Act.
[87] UETA § 3, cmt 1
[88] *Id.* § 3, cmt 3.

barriers to electronic contracting”.[89] However, because real estate transactions generally require filing with governmental offices to finalize a sale, the UETA leaves it up to the states to determine whether to “adopt an electronic filing system” or otherwise require additional “paper filing[s].”[90]

2. Related State Law Electronic Signature and Records Statutes

Three states (New York, Illinois, and Washington) have not adopted the UETA, choosing instead to implement their own unique statutes relating to electronic transactions. New York has enacted the Electronic Signatures and Records Act (“ESRA”), which recognizes that an electronic signature has the same validity and effect as a handwritten signature.[91] Like the UETA, the ESRA applies only to certain transactions and generally does not apply to transactions that involve: (i) laws relating to wills, trusts, powers of attorney, or health care proxies; (ii) negotiable instruments and other instruments of title where possession of the instrument confers title; and (iii) any other document that the New York State Office for Technology has specifically identified.[92] The ESRA adopts the UETA’s definition of an electronic signature and provides that “[a]n electronic record shall have the same force and effect as those records not produced by electronic means.”[93] Additionally, the ESRA states that an “electronic record” includes any “information, evidencing any act, transaction, occurrence, event, or other activity, produced or stored by electronic means and capable of being accurately reproduced in forms perceptible by human sensory capabilities.”[94]

In much the same way as New York, Illinois also recognizes the legal effect and validity of electronic records and signatures under the Electronic Commerce Security Act (“ECSA”).[95] Under the ECSA, an electronic signature is a signature that is both in electronic form and attached to, or logically associated with an electronic record.[96] As with UETA and ESRA, the ECSA generally does not apply to transactions that involve: (i) laws governing wills, trusts, powers of attorney, or health care proxies; (ii) negotiable instruments and other instruments of title where possession of the instrument confers title.[97]

Washington further recognizes that a digital signature satisfies the legal requirements for a signature under the Washington Electronic Authentication Act (“EAA”).[98] Under the EAA, a digital signature is a process used to attach a unique digital code to an electronic message. The signer uses a private key, a code used to encrypt or decrypt a message, to sign the electronic record. The recipient of the electronic record can then use the signer’s public key to verify whether the digital signature is valid, or the message has been altered since it was signed.[99]

[89] *Id.*

[90] *Id.*

[91] N.Y. State Tech. § 304.

[92] *Id.* § 307.

[93] *Id.* § 302.

[94] *Id.*

[95] 5 Ill. Comp. Stat. 175/5-110.

[96] *Id.* 175/5-105.

[97] *Id.* 175/5-115(b).

[98] Wash. Rev. Code § 19.34.300(1).

[99] *Id.* § 19.34.020(11).

However, neither the ESRA, ECRA, nor the EEA expressly provide for, or address, the automatic execution of an agreement via an electronic agent. These three statutes do not directly address the creation of electronic contracts via automated means.

3. The E-Sign Act

To harmonize the fractured approach taken by U.S. states, in 2000, Congress passed the E-Sign Act. Like the UETA, the E-Sign Act broadly states that electronic signatures and contracts maintained as electronic records—which are involved in "any transaction in or affecting interstate or foreign commerce"—cannot be denied enforceability or legal effect simply because they were conducted through electronic means.[100] Under E-SIGN, an electronic signature includes any "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."[101] And an "electronic record" covers any record "created, generated, sent, communicated, received, or stored by electronic means."[102]

The E-Sign Act also contemplates the use of "electronic agents" by parties, defining the term to include any "computer program" 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."[103] If parties use an "electronic agent," a contract may not be denied legal effect "so long as the action of any such electronic agent is legally attributable to the person to be bound."[104]

Except under limited circumstances, the E-Sign Act preempts state laws governing written contracts that affect interstate or foreign commerce.[105] However, the E-Sign Act contains an "exemption to preemption" section, which provides that state law may "modify, limit, or supersede"[106] the E-Sign Act if a state has either adopted the UETA, or has specified "alternative procedures or requirements"[107] that satisfy its particular requirements. Such procedures or requirements may not, according to the Act, expand the legal status or effect of the specific technology associated with "storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures."[108]

Even though the E-Sign Act employs similar language and provisions as UETA, the E-Sign Act provides for stronger consumer protections. Under the E-Sign Act, electronic records may be used to satisfy any law that requires that records be provided to consumers "in writing" only if the consumer has affirmatively consented to the use of the electronic records, and has not

[100] 15 U.S.C. § 7001(a).

[101] *Id.* § 7006(5).

[102] Hamdi Halal Market LLC v. United States, 947 F. Supp. 2d 159, 164 (D. Mass. 2013).

[103] 15 U.S.C. § 7006.

[104] *Id.* § 7001(h).

[105] *Id.* § 7002.

[106] *Id.*

[107] *Id.* § 7002(a)(2)(A).

[108] *Id.* § 7002(a)(2)(A)(ii).

withdrawn consent (the “E-Sign Consumer Consent Process”).[109] In such circumstances, the electronic record provider must deliver a clear and conspicuous statement of certain information (collectively, the “E-Sign Consumer Consent Disclosures”).[110] Moreover, the consumer must consent electronically or provide consent electronically, in a manner that “reasonably demonstrates” that the consumer can access information in the electronic format that will be used to provide the information.[111]

Thus, any in-person transaction which concludes in a paper agreement to engage in business electronically should be followed up by an electronic confirmation and consent—which must occur before any information that is required to be provided “in writing” is delivered. What satisfies the requirement is subject to interpretation: One view is that the reasonable demonstration test is flexible and can be satisfied by a consumer’s e-mail confirming that the consumer can access the electronic records or a consumer’s acknowledgment or affirmative response to a provider’s query asking if the consumer has the necessary hardware and software.[112] However, the more conservative view is that the consumer must demonstrate that they can access the information through an actual test using the electronic format in which the information will be delivered.[113]

4. Analysis Under UETA, E-Sign, and Related State Statutes

Under the UETA, E-Sign Act, and related state statutes, legal agreements relying on a smart contract would likely withstand a challenge on the grounds of enforceability. Under these statutes, a blockchain should qualify as an “electronic record,” due to the fact that a blockchain can be used, in part, as a record keeping system and is generated, sent, communicated, received, and stored via electronic means. The UETA has been interpreted to include databases,[114] the closest analogy to a blockchain.

The use of a private key to sign a transaction involving a smart contract also should readily qualify as an electronic signature. As with our analysis above, none of the aforementioned statutes strictly define what qualifies as a valid signature. Due to these statutes broad definitions, numeric codes or public-private key combinations should serve as an “electronic signature” and be deemed sufficient to establish the identity of parties relying on a smart contract.[115]

[109] 15 U.S.C. § 7001(c)(1). Several states have incorporated the requirements of the E-Sign Consumer Consent Process into their adoption of UETA. See, for example, N.J. Stat. Ann. § 12A:12-21.

[110] *Id.* A “consumer” is, for purposes of the E-Sign Act, “an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.” *Id.*

[111] 15 U.S.C. § 7001(c)(1)(C).

[112] 146 Cong. Rec. S5282 (daily ed. June 16, 2000).

[113] 46 Cong. Rec. S5215, S5216 (daily ed., June 15, 2000).

[114] Godfrey v. Fred Meyer Stores, 202 Or. App. 673, 692, 124 P.3d 621, 631 (2005) (noting that “entering . . . [a] statement into an electronic database seems to be an action of a different quality than physically taking pen to paper to record the statement. However, it is a distinction without a difference” under the UETA);

[115] *See* Stephanie Curry, Washington’s Electronic Signature Act: An Anachronism in the New Millennium, 88 Wash. L. Rev. 559, 569 (2013).

Moreover, under the UETA and E-Sign Act, a smart contract would fit neatly into both statute's definitions of an "electronic agent." A smart contract can be reasonably construed as an automated means to "initiate an action or respond to . . . performances in whole or in part, without review or action by an individual."[116] As such, even if the smart contract effectuated performance obligations without the express review of contracting parties, the agreement would still be deemed enforceable.

Yet, there are several hurdles when squaring smart contracts within existing U.S. e-signature statutes. First, the E-Sign Act and UETA emphasize the need for clear, voluntary consent between parties to use electronic records and signatures before conducting a transaction electronically. Although an express agreement is not strictly required—especially in business-to-business transactions—and an agreement may be implied or determined from relevant facts and circumstances, a standard contract written in legal prose could readily manifest parties' intent to use smart contracts to govern their transaction and would limit potential ambiguity and the risk of an enforceability challenge.

Second, for consumer transactions involving smart contracts which implicate the E-Sign Consumer Consent Process, such transactions would need to be wrapped in a system capable of providing necessary disclosures to consumers. Such a system would need to clearly and conspicuously generate a notice of the consumers' right to receive required consumer information in writing, an explanation of the scope of each consumer's affirmative consent, and describe what types of transactions the consent applies to. If applicable, such a system would also have to include a statement affirming that the consumer's consent covers the general use of electronic records and electronic signatures in connection with a transaction.

Third, because New York, Illinois, and Washington do not expressly recognize that contracts can be formed via an "electronic agent," there is a question as to whether an automated technical system—like a smart contract—will be covered by each state's respective electronic signature statutes. Contracting parties in these three states could argue that New York, Illinois, and Washington law is governed by the E-Sign Act when it comes to the use of "electronic agents," but the failure of the state statutes to address the use of "electronic agents" creates some ambiguity in these three states.[117]

III. Recent State Law Amendments Relating to Blockchain Technology and the Need for Additional Legislation

Despite the fact that the statute of frauds, U.C.C., UETA, and E-Sign Act likely would accommodate the use of smart contracts in a range of transactions, over the past several years, multiple states have begun to pass laws aimed at clarifying the enforceability of smart contracts in the context of legal agreements, presumably in an attempt to attract potential entrepreneurs

[116] UETA §2(6); 15 U.S.C. § 7006(3).

[117] *Id.* § 7002 (explaining that a "State statute, regulation, or other rule" may only "modify, limit, or supercede" the E-Sign Act if the state "specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records" and "such alternative procedures or requirements are consistent with the [E-Sign Act]."

developing applications and services relying on blockchain technology. As of October 2018, five states—Arizona, California, Nevada, Tennessee, and Ohio—have amended the UETA specifically to make records maintained on a blockchain, "electronic records" within the meaning of the UETA.[118]

For instance, in March 2017, Arizona amended its implementation of the UETA—the Arizona Electronic Transactions Act ("AETA")—to expressly include blockchain technology in the definition of "electronic records" and "electronic signatures." Specifically, the AETA now provides that "[a] signature that is secured through blockchain is . . . an electronic signature,"[119] and "[a] record or contract is secured through blockchain is . . . an electronic record."[120] The AETA also affirmatively states that "[a] contract . . . may not be denied . . . enforceability solely because that contract contains a smart contract term."[121]

In much the same way, Nevada has expanded the Nevada Electronic Transactions Act ("NETA") to clarify that an "electronic record" includes, "without limitation, a blockchain,"[122] while not otherwise affecting the state's implementation of the UETA.

Similar to the Nevada amendment, Ohio has expanded its definition of "electronic record" and "electronic signature" under the UETA to allow for transactions recorded by blockchain technology. Specifically, the amendment states that "a record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record." It also provides that, "[a] signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature." However, these amendments are a truncated version of the originally proposed statute, which included (i) a definition of "blockchain technology", (ii) a definition of "smart contracts". As proposed, both definitions mirrored that of the Arizona statute.[123]

Further, Tennessee has amended its UETA to provide that (a) "[a] cryptographic signature that is generated and stored through distributed ledger technology is considered to be in an electronic form and to be an electronic signature." and (b) "[a] record or contract that is secured through distributed ledger technology is considered to be in an electronic form and to be an electronic record."[124]

California also has sought to accommodate blockchain technology, but did not add new language to amend the UETA, rather, it clarified in the context of its legislative counsel's digest

[118] 2017 Ariz. HB 2417 44-7061; Nev. Rev. Stat. Ann. § 719.090; 2018 Tenn. SB 1662 47-10-202; 2018 Ohio. SB 220 1306.01. Of the three states which have not adopted the UETA—Illinois and New York—have both proposed laws that define blockchain in connection with electronic records and signatures. 2018 Ill. HB5553; 2018 N.Y. SB 8858.

[119] 2017 Ariz. HB 2417 44-7061.

[120] *Id.*

[121] 2017 Ariz. HB 2417 44-7061.

[122] Nev. Rev. Stat. Ann. § 719.090.

[123] 2018 Ohio. SB 300 1306.01

[124] 2018 Tenn. SB 1662 47-10-202

on blockchain technology, that the existing law provides that an electronic record or signature satisfies the law if a record is required to be in writing.[125]

As outlined in the previous section, the broad definitions of “electronic records” and “electronic agent” contained in the UETA and E-Sign Act should accommodate the use of smart contracts to create enforceable legal agreements. Thus, the amendments enacted by these various states, are largely unnecessary and may needlessly complicate the enforceability of smart contracts by creating ambiguities within the law.

For example, in the case of Arizona, newly enacted definitions of “blockchain” and “smart contract” may prove problematic if, and when, a legal agreement relying on a smart contract is interpreted by a court, due to the definition’s use of potentially ambiguous terms and terms which may not apply to emerging blockchain technology. These amendments define a “blockchain” as a “distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth.”[126] Similarly, the California definition of “blockchain” while temporary, is defined as “mathematically secured, chronological, and decentralized ledger or database.”[127]

These definitions contain specialized and ambiguous terms such as “distributed ledger technology,” “crypto economics,” “decentralized ledger,” and “tokenless” to describe a blockchain—terms which currently lack a plain and ordinary meaning. For example, the California definition uses the term “decentralized ledger,”—an ambiguous term which has yet to be defined and will likely require significant expertise and litigation in order to carefully quantify a minimum standard of “decentralization.” Moreover, the Arizona definition defines a blockchain as an “immutable” ledger, capable of providing “uncensored truth,” even though blockchains can be modified and changed, in limited instances, and thus do not strictly fall within the ambit of Arizona’s definition.[128]

The definition of “smart contract” exhibits similar problems. The phrase is defined in Arizona and Tennessee as an “event-driven program” that “runs” on a “distributed, decentralized, shared, and replicated ledger” and can “take custody over . . . assets.”[129] A plain and ordinary interpretation of this definition would not cover a smart contract relying on a blockchain, because the term “ledger” is generally ascribed to “[a] book or series of books used for recording financial

[125] 2018 Cal. AB 2658.

[126] 2017 Ariz. HB 2417 44-7061.

[127] 2018 Cal. AB 2658.

[128] For example, Merriam Webster defines the term “immutable” as “not capable of or susceptible to change.” Immutability, Merriam Webster (Online), https://www.merriam-webster.com/dictionary/immutable. The American Heritage dictionary largely follows this definition, defining the term as “[n]ot subject or susceptible to change.” Immutability, American Heritage (Online), https://ahdictionary.com/word/search.html?q=immutability.

[129] 2017 Ariz. HB 2417 44-7061; 2018 N.Y. SB 8858; 2018 Tenn. SB 1662 47-10-201.

transactions in the form of debits and credits"[130] and not computing technology. Moreover, in current implementations of blockchain technology, smart contracts are not "run" on a blockchain. Rather, as noted above, they are "run" by miners or other validators of a blockchain-based network.

Because these state's statutes contain a number of potentially ambiguous and undefined terms, courts would need to construe these definitions with reference to the intent of the legislature, generating questions about the amendment's breadth and application. [131] At worst, a court may deem existing or future architectures for blockchains or implementations of smart contract technology to fall outside these definitions, thus limiting the scope of their respective legislation.[132]

Adding further complication, by amending state UETA legislation to broadly define blockchain-based records as "electronic signatures," as Arizona and Tennessee have, states may face the risk of preemption under the E-Sign Act. As highlighted above, the E-Sign Act is deferential to states electronic signature laws only if they are consistent with the UETA, or if "alternative procedures or requirements for the use of acceptance (or both) of electronic signatures," do not "require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures."[133] By amending states UETA to broadly define blockchains and smart contracts, states risk, under a textualist interpretation of the E-Sign Act, attributing a "*greater legal status*" than had previously been granted to the defined technology, thus enabling preemption.[134]

Therefore, if states feel compelled to adopt legislation affirming the enforceability of smart contracts (and they should not), and eliminate preemption concerns, legislatures should consider adopting a narrow approach, similar to the one taken by Nevada and Ohio. Any proposed amendment could simply affirm that a blockchain can qualify as an "electronic record." By doing so, a legislature can ensure that any digital signature recorded to a blockchain is enforceable and further ensure that a smart contract will qualify as an electronic agent, since the term is defined in reference to "initiat[ing] an action or respond[ing] to *electronic records* or performances."[135]

In terms of definitions, legislatures should adopt a broad definition of a blockchain—one that accommodates future implementations and architectures for blockchains which may emerge over time. Nevada's approach here is again instructive. Nevada has defined a "blockchain" as "an electronic record of transactions or other data which is: (i) "[u]niformly ordered"; (ii) "[r]edundantly maintained or processed by one or more computers or machines to guarantee the

[130] Ledger, Black's Law Dictionary (10th ed. 2014); Ledger, Merriam Webstbloer (Online) ("a book containing accounts to which debits and credits are posted from books of original entry"), https://www.merriam-webster.com/dictionary/ledger.

[131] Unless otherwise defined, words in an Arizona statute are construed according to their plain and ordinary meaning. U.S. Parking Sys. v. City of Phx., 160 Ariz. 210, 212 (App. 1989); A.R.S. § 1–213.

[132] Such a decision would not necessarily be fatal, however. A blockchain could still be construed as an "electronic record" under the AETA and a smart contract could still qualify as an "electronic agent," as described above.

[133] 15 U.S.C. § 7002(a)(2)(A)(ii).

[134] *See*, Riley T. Svikhart, Blockchain's Big Hurdle, 70 Stan. L. Rev. Online 100 (2017).

[135] Nev. Rev. Stat. Ann. § 719.080.

consistency or nonrepudiation of the recorded transactions or other data; and (iii) [v]alidated by the use of cryptography."[136] The "Blockchain Technology Act" introduced in Illinois, defines a "blockchain" as an "electronic record created by the use of a decentralized method by multiple parties to verify and store a digital record of transactions which is secured by the use of a cryptographic hash of previous transaction information."[137] These definitions are detailed enough to differentiate a blockchain from other database structures, but broad enough to accommodate evolving architectures of blockchain technologies without resorting to vague, ambiguous terms like "ledger."

That being said, our analysis differs for states that have not adopted the UETA. Illinois, New York, and Washington should contemplate amending their state statutes to recognize and accommodate the use of "electronic agents" to engage in commercial transactions. Such an approach would harmonize these state statutes with the UETA and E-Sign Act and reduce any ambiguity around the use of a technological systems to assist with the execution of contractual performances and or whether the E-Sign Act could preempt these state laws.

IV. Conclusion

U.S. law largely accommodates the use of blockchain-based smart contracts to create binding and enforceable legal agreements, with limited exception. Under the statute of frauds and the U.C.C., parties should be able to rely on a smart contract to create enforceable legal agreements, if the smart contract outlines the material terms of the parties' arrangement and if the parties digitally sign the agreement through some volitional act. Enforceability concerns are decreased if parties incorporate, by reference, a smart contract, and rely on a "hybrid" contract that contains standard legal prose and references to relevant smart contract programs.

Even if a legal agreement relying on a smart contract somehow is deemed not to satisfy the statute of frauds or the writing requirements of the U.C.C., parties attempting to challenge the enforceability of any such contract will face an uphill battle thanks to the broad provisions of the UETA and E-Sign Act. These statutes likely will apply to contractual arrangement involving smart contracts, because a blockchain should qualify as an "electronic record" and because a smart contract should qualify as an "electronic agent."

As such, recent state amendments to the UETA are largely unnecessary. Indeed, the varying definitions of blockchain, for example, may create unintended roadblocks to innovation by creating unnecessary ambiguities and litigation. At most, New York, Illinois, and Washington should consider amending their state statutes to permit contracting via an "electronic agent."

[136] Nev. Rev. Stat. Ann. § 719.090.

[137] 2018 Ill. HB5553.