THOMSON REUTERS

Westlaw®

Smart Contracts Lead the Way to Blockchain Implementation

By Jonathan A. Beckham and Maria Sendra, *Greenberg Traurig**

MARCH 4, 2019

OVERVIEW - SMART CONTRACTS IN THE BLOCKCHAIN ECOSYSTEM

"Smart contracts" constitute a significant component of the blockchain universe. They are comprised of limited contract terms representing an agreement between two parties and are composed in source code rather than natural language. A smart contract self-executes when conditions to execution that have been included as part of the smart contract code have been fulfilled. Smart contract coding may be correlated with data sets from a blockchain platform and external data sets that deliver data through interfaces referred to as "oracles." As such, the smart contract adds the possibility of attaching customized, automated functions or processes to blockchain platform.

There are many examples of functions that may be addressed via smart contracts. For instance, an interest rate swap may be executed via smart contract. Records pertaining to the parties and their transaction terms (e.g. notional principal amount, interest rate position, contract duration, account information) may be stored on as a blockchain record. External interest rate data may be delivered to the blockchain platform via an "oracle" interface and processed by application of the smart contract. Interest rate data processed by smart contract terms would trigger automated settlement and payment to one of the swap parties.

The importance of smart contracts to blockchain implementation is evident. By adding flexible options for the development of functional process, smart contracts offer potential outcomes to facilitate the replacement of existing or legacy systems with blockchain solutions. Various parties from industries such as financial services, health care and retail have undertaken plans to introduce blockchain and smart contracts solutions, which may eventually replace legacy information technology solutions with blockchain solutions. They have also benchmarked legacy system functionality and performance against blockchain solutions. The flexibility engendered by smart contracts, as described above, suggests that blockchain solutions may eventually replicate the full functionality of legacy systems.

The marketplace appears to value the potential for smart contracting. One of the leading cryptocurrencies, Ether has distinguished itself from Bitcoin and other cryptocurrencies based upon the capacity of its underlying platform (Ethereum) to accommodate smart contract configurations. *See* Alyssa Hertig, "How do Ethereum Smart Contracts Work?" CoinDesk (https://www.coindesk.com/information/ethereum-smart-contracts-work/) However, risk factors relating to smart contracts could have a material impact on blockchain adoption and implementation. A programming error in the DAO platform resulted in a loss of $53 million in cryptocurrency and led to a "fork" in the currency as a remedy for the loss. *See* Larry D. Wall, "'Small Contracts' in a Complex World,' Notes from the Vault," Federal Reserve Bank of Atlanta (July 2016) (https://www.frbatlanta.org/cenfis/publications/notesfromthevault/1607) (last visited on 12/10/2018). Cryptocurrency funds totaling $150 million in value locked up and became inaccessible due to smart contracts coding errors and vulnerabilities. *See* Charlie Osborne, "Poor Smart Contract Coding Exposes Millions of Dollars in Ethereum," ZDNet, February 23, 2018 (http://www.zdnet.com/article/smart-contracts-leave-millions-of-dollars-in-ethereum-vulnerable/) (last visited on 12/10/2018). Security breaches of cryptocurrency smart contracts have resulted in the theft of cryptocurrency tokens. Hackers obtained access to a private key of the smart contract of a cryptocurrency, KICKICO, and users funds were compromised totaling $7.7 million in value. *See* Blockchain News, "Another ICO Hacked: KICKICO Loses $8 million after Smart Contract Breach" (July 27, 2018) (https://www.ccn.com/another-ico-hacked-kickico-loses-8-million-after-smart-contract-breach/) (last visited on 12/10/2018). Additionally, hackers managed to break into a Bancor wallet for smart contracts, through which they stole cryptocurrency tokens valued at $23.5 million. *See* Miguel Gomez, "Bancor Says Only Smart Contract Breached, 'Our Wallets Have Been Battle-Tested," July 23, 2018, Cyrptovest (https://cryptovest.com/news/bancor-says-only-smart-contract-breached-our-wallets-have-been-battle-tested/) (last accessed on 12/10/2018).

LEGAL CONSIDERATIONS OF SMART CONTRACTS

Commentators have posited that smart contracts differ from traditional contracts in that "the code is law"—performance is guaranteed and enforced by code, as the parties are bound to a given outcome. *Wall*, supra. They have speculated that smart contracts could lead to fewer disputes and reduce the involvement of lawyers. Notwithstanding such speculation, traditional legal principles apply to determine the legal status of any contract. *See*

Max Raskin, The Law and Legality of Smart Contracts, 1 Geo. L. Tech. Rev. 305, 308 (2017). These principles are generally determined based upon applicable state statutes and common law precedent, and involve considerations relating to formation, consideration, interpretation, performance, modification, breach and remedy. Smart contracts are no exception. Their evaluation from a legal perspective, however, requires nuanced consideration. For instance, in some cases, smart contracts may be accompanied by, and constitute the implementation of, an actual, natural-language contract – the accuracy of smart contract coding may be a factor for interpretation. In other cases, a smart contract may function as a stand-alone contract comprised exclusively of computer code.

TREATMENT OF ELECTRONIC CONTRACTS

Precedent exists for laws applicable to "digital" contracts. As natural language contracts evolved to include electronic copies, electronic signatures and other facets of the digital age, laws have been updated and interpreted to address this evolution.

The Uniform Electronic Transactions Act (UETA), a model law intended to harmonize rules governing electronic commerce transactions, has been adopted by 47 states (with modification). *See* Uniform Law Comm'n, "Electronic Transactions Act Summary," 2017 ("UETA Summary") (http://www.uniformlaws.org/ActSummary.aspx?title=Electronic%20Transactions%20Act) (last visited on 12/10/2018). UETA governs the validity of electronic signatures and grants legally binding status to electronic records and signatures, ensuring the enforceability of electronic transactions. UETA Summary, *supra*. UETA and its federal corollary, the Electronic Signatures in Global and National Commerce Act ("E-SIGN") validate the use of electronic records and signatures in place of physical documents.

Additional considerations arise with respect to smart contracts. Smart contracts, as discussed above, do not just involve electronic signatures, but involve (a) a cryptographic process to initiate the smart contract that connotes consent or signature to contract, and (b) access for each party to an executable software program, sometimes in place of written, natural language contract terms.

RECENTLY ENACTED STATE LAWS ADDRESSING SMART CONTRACTS

- Arizona enacted HB 2417 (amending the Arizona Electronic Transactions Act ("ETA")) into law in March of 2017. HB 2417, 53rd Leg., 1st Session (2017) (adding Article 5 to Chapter 26, Title 44 of the Arizona Code). The provision provides that signatures, records and contracts secured by a party through blockchain technology will be recognized as part of the ETA governing electronic transactions. The provision ensures that blockchain and smart contracts transactions will be recognized as valid and enforceable transactions. Finally, the provision provides that securing information on a blockchain will not change ownership of such information nor change its character, as personal information or otherwise, by its having been secured on a blockchain.

- California enacted SB838, amending the California Corporations Code so that privately held corporations can amend or adopt articles of incorporation that authorize the use of blockchain technology to record and track the issuance and transfer of share certificates.

- Delaware enacted amendments to Delaware General Corporation Law ("DGCL") in July of 2017. SB 69 added amendments to DGCL Sections 219, 224 and 232 and related provisions are intended to provide specific statutory authority for Delaware corporations to use networks of electronic databases (e.g. blockchain) for the creation and maintenance of corporate records. This permits the use of blockchain databases for maintaining a share ledger and for transmitting electronic [shareholder] notices pursuant to various DGCL provision. The provision does not address the use of blockchain for transactions other than for shareholder notices and share ledger recordkeeping. The blockchain ledger must be capable of being used to fulfill certain applicable requirements under the DGCL, such as printing the ledger.

- Nevada enacted Senate Bill 398 in June 2017, amending Nevada's Uniform Electronic Transactions Act so that a smart contract, record or signature created, stored or verified on a blockchain (a) may be enforceable or given legal effect, and (b) may be admitted as evidence. Additionally, a blockchain record shall satisfy any writing or signature requirement under the UETA or otherwise. The bill includes limitations on the use of blockchain to satisfy laws requiring records in a prescribed format or requiring notice for certain purposes, such as certain defaults, recalls or terminations. Finally, the Nevada legislation prohibits local governments from (i) imposing taxes or fees on the use of a blockchain or smart contract; (ii) requiring a certificate, license, or permit from such government to use a blockchain; or (iii) imposing any other requirement relating to the use of blockchain.

- Tennessee enacted Senate Bill 1662 in March 2018, amending Tennessee Code Title 47, Chapter 10, Tennessee's Uniform Electronic Transactions Act, The provisions provide that signatures, records and contracts secured by a party through blockchain technology will be deemed to constitute electronic signature and electronic record, which may be given effect in accordance with other UETA provisions based upon the context and surrounding circumstances of electronic signature or

record. The legislation further provides that contracts may not be denied legal effect, validity or enforceability because they contain smart contract terms.

- Vermont implemented 12 V.S.A. § 1913 in 2016, addressing the authentication of blockchain records for evidentiary purposes. A blockchain record must be accompanied by a declaration, made under oath, certifying as to information relating to the time of recordation and retrieval of the record, and to the creation and maintenance of the record.

- Wyoming enacted House Bill 101 in March 2018, authorizing corporations to use blockchain to create, record and store corporate records. HB 101 updates the Wyoming Business Corporations Act to authorize the creation and use of blockchain technology for (i) the purpose of storing records, (ii) the use of private keys and a digital address to identify and provide notices to a corporation's shareholder, and (iii) the acceptance of shareholder votes delivered by electronic signature.

UNIQUE LEGAL ISSUES RELATING TO SMART CONTRACTS

In order to facilitate the adoption and use of blockchain and smart contracts, programmers and blockchain-as-a-service vendors confront an opportunity to develop standards, protocols and controls that could be useful for the formation, interpretation and enforcement of smart contracts. *See* Reggie O'Shields, "Smart Contracts: Legal Agreements for the Blockchain," 21 N.C. Banking Institute 177 (2017); *and* Josh Stark, "Making Sense of Blockchain Smart Contracts," June 4, 2016 (https://www.coindesk.com/making-sense-smart-contracts/) (last visited on 02/28/2018). Such standards, protocols and controls will be shaped by, and in turn will shape, laws and regulations governing smart contracting. Given that blockchain and smart contracts laws are in their nascent stages, below is a discussion on legal considerations relating to smart contracts that may require attention, whether from state legislatures or smart contract parties as they license and procure services from blockchain-as-a-service vendors.

1. Contract Formation

A web of statutory codes and common law cases dictate whether a contract, electronic or otherwise, constitutes an enforceable agreement. Enforceable contracts generally require notice of applicable contract terms, mutual assent (offer and acceptance) and consideration.

- **Scope of the Parties' Agreement.** Various state laws require certain contracts to be in writing pursuant to a statute of frauds requirement. Otherwise, a contract that is not in writing can be enforced based upon one party's reliance on a commitment made by the other, or the parties' course of conduct. Terms of a natural language contract relating to a transaction that is governed by a smart contract may conflict with the smart contract. The parties may intend for the natural language contract to govern in case of a conflict; however, traditional legal principles do not appear to grant precedence of one form of contract over the other.

- **Contract terms notice requirement.** Whether electronic contract terms constitute sufficient notice of contract terms has been addressed in the context of shrink wrap licenses. *See* O'Shields, "Smart Contracts," *supra* 186-187. Contract terms must be conspicuously available to contracting parties. This may include requiring a party of click on an "agree" button and an express warning to a party that continuing with the transaction would bind that party to the contract. While various states are now implementing legislation confirming the enforceability of smart contract as a form of electronic signatures, such provisions have not typically addressed the manner in which contracting parties receive notice of smart contract terms. What constitutes conspicuous notice in the context of blockchain and smart contracts is to be determined.

- **Mutual Assent.** Based upon state legislation highlighted above relating to smart contracts, a party's consent may be evidenced by its submission of public and private key information. A signature must be "secured" through blockchain technology. Future legislation and/or contracting protocols might consider additional standards and protocols for authenticating signatures. Protocols for agency representation, notarization, and other elements relating to contract assent require consideration—the development cryptographic, consensus-based processes for agents, notaries and execution of documents could be useful. A blockchain consortium, R3, has introduced methods for notarization of smart contracts. Additionally, the Nebraska legislature has introduced legislation authorizing digital notarization for distributed ledger solutions.

- **Statute of Frauds.** Legislatures have recognized electronic contracts and now smart contracts secured on a blockchain as sufficiently reduced to tangible form for the purpose of satisfying the statute of frauds. Uniform protocols, statutes and regulations expressly relating to acceptable methods of setting forth a smart contract in "tangible" form, for evidentiary or other purposes, warrant consideration. Protocols could require natural language translations of or addendums to smart contracts.

2. Interpretation, Performance and Termination of Smart Contracts

Blockchain records and smart contracts are typically intended to be immutable. However, from time to time, circumstances may arise, whether pursuant to a dispute, error, judgment or order, or the agreement of the parties, for which a smart

contract or blockchain record may require amendment, modification, rescission or termination.

- **Defenses to Enforcement.** A party may argue a number of defenses to the enforceability of a contract, to include mistake, misrepresentation, duress, violation, unconscionability and illegality. Some commentators have suggested that smart contracts are less prone to ambiguity since programming languages recognize fewer terms than humans. *See* Raskin, "Law and Legality of Smart Contracts," *supra* at 324. However, smart contracts may require translation from executable language to natural language and vice versa. Smart contracts must be capable of remedy based upon the foregoing defenses. The parties should consider risks associated with smart contract coding and translations of code to and from natural language. Additionally, lawmakers and the parties might anticipate the need to configure possible mechanisms to unwind or reverse a smart contract.

- **Smart contract errors.** Smart contracts may contain costly mistakes or errors that do not reflect the intent of the parties, and/or that reflect the input of erroneous data, the application of erroneous logic to a calculation, or premature execution of an automated function. The parties might consider protocol and governance mechanisms for correcting or replacing code and/or reversing or offsetting executed transactions.

- **Performance.** While courts may recognize partial performance or substantial performance of an obligation as constituting satisfaction of a party's obligations, an executable computer program may not recognize this result. A smart contract must follow a binary calculation to determine whether criteria has been satisfied. Modification of the outcome of the execution of a smart contract may be required from time to time based upon the application of legal principles.

- **Bankruptcy / Insolvency; Early Termination.** A smart contract may constitute an executory contract for bankruptcy purposes. As such, a smart contract may be subject to termination by a debtor in accordance with applicable bankruptcy or insolvency rules. Additionally, a contractual obligation pertaining to a smart contract may be terminated in accordance with applicable contract terms due to a material breach or other early termination right. The parties may consider protocols, further described below, relating to early termination.

CFTC AND SEC CONSIDERATION OF SMART CONTRACTS RISKS AND LIABILITIES

Smart contract applications may have a nexus to blockchain and other platforms utilized for trading or investment purposes. In 2018, the Commodities and Futures Trading Commission released its "Primer on Smart Contracts." See Lab CFTC, A Primer on Smart Contracts, dated November 27, 2018 (https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf) (the "CFTC Primer"). The CFTC Primer considers that a smart contract application used by an entity registered with the CFTC may constitute a product subject to CFTC jurisdiction. The CFTC Primer elaborates on prohibited activities for such contracts, and provides an overview of operational, technical and cybersecurity risks for smart contracts, as well as certain means by which smart contracts may be utilized or exploited to engage in fraud and manipulation The CFTC suggests that the development of governance standards as a means to combats risks and problems associated with smart contracts.

Recently, a CFTC Commissioner commented on the hypothetical application of the Commodities Exchange Act to smart code developers. Remarks of Commissioner Brian Quintenz, 38th Annual GITEX Technology Week Conference (October 16, 2018) (https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16). Commissioner Quintenz, in addressing how regulators apply existing legal paradigms to novel technologies not contemplated when those laws were adopted, considered who might who might be responsible for ensuring that activity on the blockchain complies with the law. He evaluated the potential liability of blockchain core developers, users and miners, and ultimately concluded that smart contract code developers who might reasonably foresee violations of CFTC regulations stemming from smart contract usage may be construed as "aiding and abetting" such violations.

The Securities Exchange Commission has addressed the applicability of registration requirements to a smart contracts-based platform that allowed buyers and sellers to trade digital assets in secondary market trading. In re Zachary Coburn, Exchange Act Rel. No. 84553, dated November 8, 2018 (https://www.sec.gov/litigation/admin/2018/34-84553.pdf). The online trading platform's smart contracts consisted of coded functions that allow for the trading of Ether-based tokens. The SEC found that the online platform constituted an "exchange" under § 3(a)(1) of the Exchange Act and Rule 3b-16(a). The SEC has emphasized that market participants must still adhere to our well-established and well-functioning federal securities law framework when dealing with technological innovations. See SEC Statement on Digital Asset Securities Issuance and Trading, dated November 16, 2018 (https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading).

CONCLUSION

Smart contracts represent a significant corollary to blockchain and distributed ledger technology systems, adding the potential for automated processes and functionality. Existing federal law recognizes the enforceability of smart contracts.

State laws have been enacted in several jurisdictions and are under consideration in additional jurisdictions to ensure that smart contracts are recognized as enforceable instruments. Some states have considered authorization for digital notarization techniques involving smart contracts and blockchain technology. These measures are intended to ensure that governments facilitate the continued adoption and use of smart contracts and blockchain technology. Additional considerations may arise under the law, as developers, contracting parties and, subsequently, courts, may grapple with novel issues, such as the interplay between coded contracts and natural language contracts, and legal rights such as rescission and equitable enforcement. Smart contract applications may facilitate trading or commercial exchanges involving transactions and parties subject to the jurisdiction of the Securities and Exchange Commission or Commodities and Futures Trading Commission.

This article first appeared in Westlaw's publication entitled Payment Systems and Electronic Fund Transfers Guide. The publication is part of the Emerging Areas of Practice Series – a new publishing initiative which reduces product to market time to cover emerging areas of the law as they develop. New documents are loaded to Westlaw on a rolling basis as received and content is updated quarterly.

ABOUT THE AUTHORS

Jonathan A. Beckham is of counsel in Greenberg Traurig's Northern Virginia office. His practice focuses on sophisticated, cross-border commercial and corporate transactions, with an emphasis on technology transactions, outsourcing and general corporate matters. He negotiates transactions relating to the cloud infrastructure and network-build transactions, the license of cloud services and software to leading financial institutions and other enterprise customers, data-as-a-service and IoT-platform license transactions, and patent license and joint development agreements. Jonathan negotiates and advises on intellectual property and technology matters for merger and acquisition and other corporate finance and joint venture transactions.

Maria Sendra is a shareholder in Greenberg Traurig's Silicon Valley office. She has built a disruptive technology and finance practice that helps companies to scale innovation globally by leveraging capital markets, private equity, and technology relationships in key jurisdictions around the world. She has managed international teams of over 500 experts, in helping to globally scale start-ups, as well as Fortune 500 companies, venture capital, private equity and investment banking efforts in disrupting a wide variety of industries, including data analytics, finance, IoT, energy, cleantech, biotechnology and genomics, digital healthcare, entertainment, consumer goods, real estate, digital and smart cities, blockchain, cryptocurrencies, retail and e-commerce sales and scaled revenue strategies. She has structured and managed domestic and international manufacturing, R&D, distribution, financing, licensing and strategic alliances and businesses linking California innovation to financial markets in New York, London, all over Europe, Latin America, Asia and the Middle East.