Bloomberg Law
Tech & Telecom

Blockchain ‘Smart Contracts’ – A New Transactional Framework

*By **Laura E. Jehl** and **Brian Bartish***
Baker & Hostetler LLP

This article, the third in a series, explores applications of blockchain technology.

With the growing buzz around blockchain technology, many organizations are in a race to position themselves as early adopters and leaders in the space. For these organizations, one of the more exciting blockchain applications is the promise of increased efficiency and reduced costs in the transacting process through so-called “smart contracts” – which are actually neither “smart” nor necessarily true legal contracts. Smart contracts are automated programs that encode transactional logic for self-execution and rely upon decentralized cryptographic methods to effectuate enforcement. Regardless of one's opinion of their name, or their legal status, smart contracts are garnering a significant amount of attention and investment due to their ability to radically transform the way parties transact with one another.

♦ What are smart contracts?

Smart contracts actually predate the creation of blockchain technology, as the term “smart contracts” was first coined by computer science and legal researcher Nick Szabo in the mid-1990s. Szabo defined a smart contract as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises.” He offered an analogy of the vending machine to illustrate his premise that the entire environment of the transaction could be created within the purview of a machine. In stocking the vending machine, the owner has created an offer, which is accepted when a buyer inserts cash and makes a selection. The code running the machine then takes over to perfect performance by verifying the currency input, dispensing the buyer's selection, and returning any required change. While Szabo's initial vision of smart contracts promised modest gains in transactional efficiency through automation, the advent of blockchain technology has created a number of significant new benefits, perhaps chief among them the ability to create trust between parties operating in a trustless environment that does not rely on a centralized institution, government, or other middleman.

♦ How do smart contracts operate?

Smart contracts rely on code deployed on a blockchain to automatically execute the terms of an agreement. This is where smart contracts begin to depart from traditional contracts, i.e., agreements embodying certain terms to be fulfilled by parties and given the force of law to incentivize performance. In contrast, smart contracts can be viewed as “autonomous agents” designed to execute the logic of an agreement through code that responds to specific messages or transactions. In computational terms, smart contracts are programs that can execute an arbitrary, or open-ended, array of user-specified state transition functions, including performing calculations and storing information. These alter the collective status, or state, of the underlying system, which embodies the entire history of preceding events and the way those events bear upon circumstances such as the ownership of outstanding currencies, the location of goods in transit, or the status of voting rights. The programs function as cryptographic “boxes” that contain value or information and that can only be unlocked in response to certain predefined conditions. Smart contracts, therefore, aren't truly smart, but rather deterministic.

While not as "smart" as advertised, blockchain-based smart contracts represent an evolution of the underlying bitcoin technology, requiring more powerful platforms and more robust programming languages. The Ethereum Virtual Machine, or simply Ethereum, is the best-known of these platforms. Ethereum emerged with its own programming language, Solidity, specifically designed to encode logic into smart contracts. Ethereum and Solidity offer important advancements over the bitcoin architecture, as both were designed to be "Turing-complete," meaning that they can encode any computation that can be conceivably carried out, including infinite loops. This capability becomes important as the complexity of smart contracts increases, particularly when a smart contract calls on another smart contract as an independent data source or a verifier of real-world events (often referred to as an "oracle"). For example, smart contracts involving financial derivatives may rely on an external source of data, such as the value of the dollar or the Nasdaq index, which can be fed to the derivatives contract through a separate smart contract deployed specifically for calculating those functions. The fact that Solidity is Turing-complete, however, may expose users to infinite loops in contract execution that can cause significant delays and waste both computational and financial resources. Ethereum attempts to manage this type of "denial of service" threat through its transaction structure. Each Ethereum transaction consists of:

- the message recipient;
- the cryptographic signature of the sender;
- an amount of ether (the cryptocurrency used on Ethereum) to transfer;
- an optional data field;
- a "startgas" value, which represents the maximum number of computational steps that a transaction can take when executing; and
- a "gasprice" value, which represents the price per computational step that the sender pays to the miner in order to publish the transaction to the blockchain.

In the event that a transaction "runs out of gas" before completing its execution, the participating nodes and the entire blockchain revert to their previous states, but the miner (i.e., the node that earns the right to publish the block containing the transaction) still collects the gasprice transaction fee. This design, however, is not foolproof against all malicious attacks and still presents some significant risks due, in part, to simple programming error.

Another risk was exemplified by the so-called Decentralized Autonomous Organization (DAO), where a number of Ethereum users joined together to create a sort of crowd-funded venture capital fund where members could vote to invest the DAO's funds in a number of projects. This early attempt at an organization managed entirely through smart contracts ended in ignominy, however, as an attacker exploited flaws in the logic of the underlying smart contracts to siphon off nearly $50 million in ether. The funds were recovered, but only after Ethereum leaders convinced a majority of nodes on the platform to implement a "hard fork" – essentially an operation that reverted the state of the network to what it was prior to the theft. This hard fork, however, required the users to abandon the original network, which still exists under the name Ethereum Classic. The DAO hack served as a lesson that many of the purported strengths of the blockchain architecture, such as its immutability, may be detrimental in certain contexts. Users should therefore carefully consider whether the blockchain will increase the efficiency of transactions or subject them to heightened or unnecessary risks.

♦ Smart contract use cases

Despite the risks, smart contracts offer a number of exciting potential use cases. The developers of Ethereum envisioned a broad array of uses, such as financial derivatives for crop insurance, savings wallets, wills, employment contracts, and peer-to-peer gambling. Smart contract use cases extend beyond the purely financial, as they offer a potential solution to coordination failures among transacting parties. They also offer avenues for experimentation with decentralized governance structures for software development, project management, and entire business organizations.

Unlike the early days of Ethereum, corporations are now investing in smart contract pilots and setting up joint ventures to work on the technology. In 2017, AIG partnered with IBM to create a smart contract multinational insurance policy for Standard Chartered Bank PLC. The policy operates through multiple smart contracts, covering a main policy for Standard Chartered's U.K. headquarters and local policies for affiliates in the U.S., Singapore, and Kenya, which communicate to share data and documents. Also in 2017, French insurer AXA started testing Fizzy, a flight-delay insurance product that leverages smart contracts on the Ethereum blockchain. The smart contracts are connected to global air traffic databases so that as soon as a flight is delayed more than two hours, the smart contract triggers compensation to the insured traveler.

One of the most oft-cited implementations of a smart contract is supply chain management, in which a contract or series of contracts is part of a system that automatically controls the shipment of goods and payments through all stages of the logistics cycle. IBM recently announced a new joint venture with Danish firm A.P. Moller-Maersk – the world's largest container shipping firm, handling roughly one in seven containers shipped globally – that will implement smart contracts as part of a comprehensive strategy to digitize the global supply chain. Their goal is to drive down expenses and increase the speed of the end-to-end shipping process by using smart contracts to automate costly customs clearance and approval requirements.

Beyond the corporate world, governments are also experimenting with the technology. Sweden's land registry authority, the Lantmäteriet, is testing a system for real estate transactions and mortgage deed processes. This would allow buyers and sellers to strike a deal using a smart contract connected to a private blockchain, which reduces the need for paperwork and provides greater transparency in chain of title. One of the hurdles in the Lantmäteriet's road map is a legal issue: validity of digital signatures for real estate contracts. Elsewhere around the globe, Dubai is undertaking a comprehensive digital transformation that would migrate all visa applications, bill payments, and license renewals to blockchain technology by 2020.

While blockchain-based smart contracts are still in a state of infancy and their risks are not always fully anticipated, the interest in their applications to the commercial sector has intensified development efforts. Hyperledger, Project Accord, and the Enterprise Ethereum Alliance have already gained a number of influential supporters from various fields.

Hyperledger is a membership-based organization with the objective of advancing cross-industry blockchain technologies. It incubates and promotes a number of tools including Hyperledger Burrow – a smart contract machine contributed by smart contract startup Monax and co-sponsored by Intel – which executes Ethereum smart contract code on a permissioned virtual machine. Hyperledger has more than 100 members, from tech companies to banks and academic institutions to commercial industry groups.

The Accord Project is an open source software initiative established with Hyperledger, the International Association for Contract & Commercial Management, and the W3C, a web standards body. One of its projects, Cicero, aims to provide lawyers and business professionals with a system for turning paper-based, legally binding agreements into legally binding smart contracts. The Accord Project's membership consists of big law firms, startups, venture capital firms, and other organizations.

More than 150 organizations from a range of industries – including software, infrastructure, financial services, manufacturing, and law – signed on to the Enterprise Ethereum Alliance, launched in February 2017. Formed with the goal of connecting business leaders, startups, academics, and vendors with Ethereum subject matter experts to establish a road map for enterprise adoption, the Ethereum Enterprise Alliance counts Microsoft, JPMorgan Chase, Mastercard, BP, ING, and Deloitte among its members.

Propelled by the strong interest of these well-funded industry leaders, smart contracts are increasingly appearing on legislative agendas. Arizona and Nevada have recently passed laws that promote the legal enforceability of smart contracts, and Florida appears poised to do the same. Much like smart contracts themselves, the gears of progress propelling these efforts appear poised to self-execute.