

## Get Smart: Automating Business Agreements With Blockchains And Smart Contracts

By Matt Savare and Kurt M. Watkins

- Unless you have been living under a rock for the last year, you have heard and read about Bitcoin, which is electronic cash supported by a peer-to-peer network of computers linked via the Internet. Although Bitcoin receives the lion's share of the press – and is the most valuable cryptocurrency by market capitalization – another such network, Ethereum, is powering a transformation in the way business is conducted. Ethereum is an open source blockchain platform that utilizes a Turing-complete programming language (i.e., capable of computing anything that is computable given sufficient resources) that enables the creation of decentralized applications and “smart contracts.” Without being hyperbolic, smart contracts, which automate business processes using blockchain technology, have the potential to disrupt and revolutionize the provision of business services the same way robots did manufacturing.
  - The shared ledger is the information stored on each of the nodes. Any transaction, or specified group of transactions, is grouped into a “block” of information, and each block is cryptographically linked (or chained) to the adjacent blocks, hence the name blockchain. Together, these transactions and the blocks that store and connect them are the shared ledger. Each node powering the blockchain maintains an identical copy of the shared ledger in its entirety (i.e., each block on the blockchain from the very first block to the very last one). Because reconciliation of the shared ledger is automatic and simultaneous across the entire blockchain, the shared ledger is a single store of truth in an otherwise trustless, decentralized environment.
  - The consensus mechanism is the algorithm the blockchain uses to automatically guarantee properly functioning nodes and data transactions. There are a variety of consensus algorithms (e.g., proof-of-work and proof-of-stake), but each one ensures the consistency of the data across all the nodes in a blockchain and ensures those nodes are behaving normally. Should any one node be compromised, the algorithm will recognize it as behaving abnormally and instruct the remaining nodes to take corrective measures. Further, if an improper data transaction occurs, the additional security provided by the cryptographic links will forbid the impropriety.
  - The virtual machine is what processes the instructions for the blockchain. It is, in essence, the computer that would exist if all the nodes of the blockchain were contained in a single computer.
- The first functional platform to realize these advantages for broad application was Ethereum. Although Ethereum issues tokens (Ether) that can be used for payments, its core value emanates from the ability of its virtual machine to process data transactions and decentralized applications rather than simply exchange tokens, like Bitcoin does. This enhanced functionality enables Ethereum to power and process smart contracts, presenting businesses with two critical advantages: a massive reduction in overhead and greater reliability than current technology models.
- ### Rise of the (Decentralized) Machines
- Today, businesses typically store their information on centralized servers (their own or those of cloud service providers) and share that data with the central servers of third parties, such as banks, vendors, and customers. Such a centralized-server model has three fundamental weaknesses: (1) the costs and inefficiencies associated with having to reconcile data sets; (2) the vulnerability of the central locations to cyber-attacks; and (3) the necessary provision of sensitive data to third parties who facilitate information sharing. A new model based on the blockchain has arrived.
  - Blockchain technology obviates the need for centralized servers. Instead, data is transacted and stored in a decentralized or “distributed” fashion using the combination of four elements: nodes, a shared ledger, a consensus mechanism, and a virtual machine, which together comprise a “blockchain.”
  - Nodes are computing devices connected to the Internet and running the blockchain software. They represent the physical element of a blockchain and store all of its information. The diffusion of information across the various individual nodes is what makes the blockchain decentralized.

## Automatic for the People: The Emergence of Smart Contracts

Although there is no definitive definition of “smart contracts,” they are, at the most fundamental level, programs (or “autonomous agents” as the Ethereum white paper dubs them) that execute instructions exactly as programmed. After they are developed and deployed onto the blockchain network, smart contracts are self-executing and self-enforcing. For example, suppose a bank has decided to reap the benefits of smart contracts and created a decentralized system on the Ethereum blockchain to handle its accounting. Now, the bank wishes to issue a mortgage to a borrower. The parties agree to run their mortgage on the Ethereum network, thereby automating payments without the need to develop or license a costly proprietary system. The computer-coded terms would be stored not only by the parties mentioned, but also every other node on the blockchain. This ensures that the smart contract cannot be changed without the consent of the bank and the borrower. If the borrower does not have enough funds in his or her account, then the bank would be instantly notified and different terms could be enforced in the event of a default. And, once the borrower has paid back the mortgage, the network would update and automatically remove the debt obligation on the bank’s system. If properly programmed and linked with an available smart contract processing title documents, the final payment would automatically update the title of the home and remove the bank’s lien on the property.

Other examples abound. In the world of financial transactions, smart contracts can be programmed to execute various trades (e.g., stocks, bonds, Bitcoin) when certain conditions precedent are satisfied and without having to trust any party to perform the transactions. A supply chain blockchain can automatically track goods in real time, properly route them to the correct destinations, and remit payments to the appropriate parties along the way. An artist can track the use of his or her intellectual property in real time as well as manage those digital rights and receive payment without the long line of intermediaries that currently dominate the system (e.g., Apple’s 1/3 cut). A company can automatically track its shares, update its cap table, and administer shareholder voting. With smart contracts, these and many more processes that ordinarily require several layers of human oversight can be more easily managed, provide data in real time, reduce overhead and confusion, and create new opportunities.

However, utilizing a distributed network (public or private) requires not only retooling a business’s current environment, but also obtaining buy-in from all of the interested parties. Because smart contracts process binding transactions, a company’s counsel (in-house and/or external) should be involved with their development and deployment to ensure that the smart contracts reflect the human negotiations and do not expose the business to otherwise unforeseen legal consequences. Most critically, there must be meaningful cooperation among the parties that will use the system and the software developers who will help code them.

## Building Blocks: Creating and Deploying Smart Contracts

In order to craft and deploy smart contracts that accurately reflect the parties’ understanding, that transform the way transactions are executed, maintained, administered, and enforced, and that reliability replace standard contracts (in whole or in part), lawyers, software developers, and the interested parties to the transaction must collaborate in a number of meaningful ways.

As a preliminary issue, although smart contracts more efficiently govern transactions among the parties, a traditional contract must still govern the blockchain’s terms of use and the legal relationships and obligations among the parties. The traditional contract will set forth the terms of the software license, what law applies in the event of a dispute, where the dispute should be resolved, each party’s contribution to the production of the blockchain, what smart contracts will be deployed, and other standard terms such as representations and warranties, indemnification, and limitation of liability.

The traditional contract will also set forth what kind of platform the parties will run among themselves. Broadly speaking, the platform will be either a public blockchain, like Ethereum, or a private blockchain, like a Hyperledger project. The advantage of a public blockchain is that the platform is already built and trusted. However, it is more difficult to ensure privacy, efficient transactions times, and develop sophisticated tools on such a platform. The alternative, a private blockchain, requires more upfront investment and buy-in from the participants, as it must be customized. Either option will fundamentally do the same two things: form a universal consensus on the facts and execute actions based on that consensus. This first technical decision, as well as all those that flow from it, must anticipate the legal requirements of data storage, privacy, and the transactions to be performed on the blockchain. The parties’ legal teams are best positioned to aid in this decision.

Once the platform is built, the parties need to develop and deploy their smart contracts. Much like the creation of other customized digital applications, software developers write the code to perform specific functions and the users of the code (i.e., the various parties to the smart contract) interface with the application by providing correct inputs and access to the appropriate information. During this process, however, the developers need the support of legal specialists, who can accurately convey the legal requirements of the code as well as listen to, and work with, the developers when a straightforward method of coding for the legal parameters cannot be achieved.

To execute or go live with a smart contract, a party must “sign” the contract. Unlike in the case of traditional contracts, smart contract execution is not achieved through a handwritten or electronic signature. Rather, every party on the platform has a unique signing tool, its private key. By running its private key against a smart contract, the smart contract will execute the functions the party requires of it. This “signing” leaves an indelible imprint stating the time that the party executed the smart contract.

Finally, the terms of the smart contract are broadcast to the entire decentralized system, which automatically updates the shared ledger after reaching consensus that the transaction is valid. To ensure privacy, the terms can be “hashed,” a cryptographic process whereby the terms are given unique markers that cannot be reverse engineered.

Although smart contracts deployed on the blockchain are relatively new phenomena, they are already profoundly transforming the way we conduct business. From shipping to banking, logistics management to livestock, the legal profession to insurance, and the entertainment industry to the Internet of Things (IoT), smart contracts are becoming more widely adopted across a range of uses cases for businesses, individuals, and even IoT devices. Successful creation and deployment of these smart contracts requires smart collaboration among the various stake holders, their developers, and their attorneys.

*Matt Savare is a partner and Kurt Watkins is an associate at Lowenstein Sandler LLP, where they practice intellectual property, technology, blockchain, and privacy law.*

This article was originally published in Global Banking & Finance Review®. The original article can be found here: <http://www.globalbankingandfinance.com/get-smart-automating-business-agreements-with-blockchains-and-smart-contracts/>



## Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

**Matt Savare, Esq.**

Partner

T 646.414.6911 | [msavare@lowenstein.com](mailto:msavare@lowenstein.com)

**Kurt M. Watkins, Esq.**

Associate

T 973.597.6120 | [kwatkins@lowenstein.com](mailto:kwatkins@lowenstein.com)

---

NEW YORK

PALO ALTO

NEW JERSEY

UTAH

WASHINGTON, D.C.