Bloomberg Law Tech & Telecom

An Introduction to Blockchain Technology

*By **Laura E. Jehl**,*
Partner,
BakerHostetler

This article, the first in a series, explores the basics of blockchain technology. Future installments will examine digital currencies and non-currency applications of blockchain technology across a variety of industries.

♦ What is blockchain technology? How does it work?

Blockchain is a decentralized distributed ledger. What does that mean? Envision a standard business ledger, like your bank statement, credit card bill, or a local tax bill. The ledger records transactions, usually transfers or exchanges of assets, into or out of a particular "account," and is compiled by a central authority such as a bank or government agency. A standard ledger system requires that the central agent be trusted: if a bank verifies an electronic funds transfer, for example, that transfer is deemed to have been made even if one party or the other contends that it did not.

A decentralized ledger is a database that is synchronized across a peer-to-peer network of computers. The ledger permanently records changes to the database using cryptographic hash-linked "blocks." When a transaction occurs, a block is added to the ledger, forming a sequential chain with previous transactions, thus the name blockchain. Each block contains data from the previous block, so each transaction can be validated by computers and viewed and affirmed by consensus among the participants in the network. No single party controls the data or the information. Every party can verify the records on the ledger directly, without reliance on any central authority.

♦ What are the advantages of blockchain?

Blockchain technology offers greater efficiency, transparency and security than centralized, trust-based systems and processes.

Centralized systems can be slow and expensive, as middlemen and verification processes clog the pipes. Suppose you want to send money to a family member abroad. If you wire the funds via an intermediary (*e.g.,* your bank or Western Union), the transfer will be subject to fees for electronic funds transfer, currency exchange and more. The transaction will also likely be delayed, often several days, by mandatory waiting periods and settlement times, regulatory oversight, and will be vulnerable to diversion or corruption along the way. In contrast, anyone with a digital currency "wallet" (easily available online) can transfer bitcoin or another virtual currency from anywhere using a smartphone app. The bitcoin is sent directly to the intended recipient's wallet, pseudonymously (if the sender wishes) and without incurring fees, and the amount and addresses will be recorded on a public ledger, adding blocks to the chain. While blockchain transactions are not instantaneous, they usually take several minutes, rather than several days for standard bank transactions.

Reproduced with permission from Bloomberg Law, https://www.bna.com/bloomberglaw/. Copyright © 2017 by The Bureau of National Affairs, Inc., 1801 S. Bell Street, Arlington, VA 22202 (800-372-1033), http://www.bna.com.

Every transaction on the blockchain is visible to anyone in the computer system. Each user (known as a node) on the blockchain has a unique alphanumeric address, and everyone on the network can monitor each transaction.

Distributed ledger transactions also offer security advantages over those enabled by a central authority. Because the ledger is chronologically ordered and stored on many computers across the network, a "hack" of a distributed ledger would require simultaneous changes to data on all systems. The algorithm behind the blockchain has (thus far) been very secure. While there have been highly-publicized thefts of digital currency, those incidents involved the compromise of internet-connected digital currency organizations or exchanges, not of the blockchain itself.

♦ What's the difference between blockchain and Bitcoin?

Bitcoin was the first use of blockchain/distributed ledger technology, and the first cryptocurrency or virtual currency. Bitcoin has real monetary value, but it only exists in the ledger. It was born out of the 2008 financial crisis, and was intended to create a mechanism for anonymous online payments without need for a central authority. Although Bitcoin has been embraced as a payment method by many legitimate businesses and individuals, its relative anonymity has also led to widespread use for criminal activities such as money laundering and ransomware payments. After Bitcoin, a number of other cryptocurrencies were launched, most notably Ethereum, which created both a platform for digital currency and an engine for other applications, including so-called "smart contracts." Many — but not all — of the newer cryptocurrencies permit or require proof of a user's identity.

♦ What are some non-currency applications of blockchain technology?

New applications for blockchain technology are growing explosively across industries as diverse as financial services, venture funding, manufacturing, real estate, Internet of Things and government agencies. A few of the most promising use-cases to date include:

"Smart contracts" (which, it has been said, are neither smart nor contracts) embed code in the blockchain network which defines the conditions to which all parties to the contract agree. When, and if, required conditions of the contract are met, the contract self-executes. If a contract for the shipment of goods requires that the goods reach a destination by a certain date, when the goods are confirmed to have arrived on time the code will trigger an automatic payment. Smart contracts eliminate the costs and delays associated with middlemen.

"Provenance." Blockchain provides a secure and immutable way to establish "provenance" — where something came from and where it's been since. Questions of provenance are at the core of many legal issues — verification of title to real estate; the origin and receipt of shipped goods; ensuring the authenticity of luxury goods, art and expensive wine; or being able to identify "conflict diamonds " — to name a few. The immutable mechanisms of blockchain eliminate the need for costly audits, registrations and validation.

"Self-sovereign identity." Several promising projects are exploring the use of blockchain technology to create a "self-sovereign identity" — a single, secure and immutable identity record for each person, which is portable, cannot be taken away, and does not depend on any centralized authority. These digital identity projects offer significant opportunities to improve and streamline identification processes by creating, in effect, a permanent and secure "identity card" for everyone, including both "the undocumented" — refugees and migrants who have lost their records, as well as people from undeveloped regions with no formal identity document process to begin with — and even replacing paper passports.

Closer to home, countless data breaches at companies and government agencies holding vast databases of consumers' personal information have broken the current "user name and password" scheme for online identification. Self-sovereign identity may offer a new model: one in which the individual would control access to his or her personal data, which could be used across the internet to verify access to websites and conduct business, and could limit the use of that data to only the "minimum necessary" for each interaction. Verification of identity would become automatic for all websites rather than requiring an ad hoc procedure that must be repeated each time the user logs in.

COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC.