In Blockchain We Trust

By Michael J. Casey and Paul Vigna

What makes a blockchain a special kind of ledger is that instead of being managed by a single *centralized* institution, such as a bank or government agency, it is stored in multiple copies on multiple independent computers within a *decentralized* network. No single entity controls the ledger. Any of the computers on the network can make a change to the ledger, but only by following rules dictated by a "consensus protocol," a mathematical algorithm that requires a majority of the other computers on the network to agree with the change.

Once a consensus generated by that algorithm has been achieved, all the computers on the network update their copies of the ledger simultaneously. If any of them tries to add an entry to the ledger without this consensus, or to change an entry retroactively, the rest of the network automatically rejects the entry as invalid.

Typically, transactions are bundled together into blocks of a certain size that are chained together (hence "blockchain") by cryptographic locks, themselves a product of the consensus algorithm. This produces an *immutable,* shared record of the "truth," one that—if things have been set up right—cannot be tampered with.

Within this general framework are many variations. There are different kinds of consensus protocols. There are public, "permissionless" blockchain ledgers, to which in principle anyone can hitch a computer and become part of the network; these are what Bitcoin and most other cryptocurrencies belong to. There are also private, "permissioned" ledger systems that incorporate no digital currency. These might be used by a group of organizations that need a common record-keeping system but are independent of one another and perhaps don't entirely trust one another—a manufacturer and its suppliers, for example.

The common thread between all of them is that mathematical rules and impregnable cryptography, rather than trust in fallible humans or institutions, are what guarantee the integrity of the ledger.

It's a version of what the cryptographer Ian Grigg described as "triple-entry bookkeeping": one entry on the debit side, another for the credit, and a third into an immutable, undisputed, shared ledger.

Bitcoin showed that an item of value could be both digital and verifiably unique. Since nobody can alter the ledger and "double-spend," or duplicate, a bitcoin, it can be conceived of as a unique "thing" or asset. That means we can now represent any form of value—a property title or a music track, for example—as an entry in a blockchain transaction. And by digitizing different forms of value in this way, we can introduce software for managing the economy that operates around them.

As software-based items, these new digital assets can be given certain "If X, then Y" properties. In other words, money can become *programmable*. It's quite different from analog tokens such as banknotes or metal coins, which are agnostic about what they're used for.

What makes these programmable money contracts "smart" is not that they're automated; we already have that when our bank follows our programmed instructions to autopay our credit card bill every month. It's that the computers executing the contract are monitored by a decentralized blockchain network. That assures all signatories to a smart contract that it will be carried out fairly.

Programmable money and smart contracts constitute a powerful way for communities to govern themselves in pursuit of common objectives. They even offer a potential breakthrough in the "Tragedy of the Commons," the long-held notion that people can't simultaneously serve their self-interest and the common good.

But here's the thing: the open-source nature of blockchain technology, the excitement it has generated, and the rising value of the underlying tokens have encouraged a global pool of intelligent, impassioned, and financially motivated computer scientists to work on overcoming these limitations.

The crypto bubble, like the dot-com bubble, is creating the infrastructure that will enable the technologies of the future to be built.