BLOCKCHAIN

In blockchain we trust

To understand why blockchain matters, look past the wild speculation at what is being built underneath, argue the authors of The Age of Cryptocurrency and its newly published follow-up, The Truth Machine: The Blockchain and the Future of Everything.

By Michael J. Casey & Paul Vigna

April 9, 2018

SELMAN DESIGN

The dot-com bubble of the 1990s is popularly viewed as a period of crazy excess that ended with hundreds of billions of dollars of wealth being destroyed. What's less often discussed is how all the cheap capital of the boom years helped fund the infrastructure upon which the most important internet innovations would be built after the bubble burst. It paid for the rollout of fiber-optic cable, R&D in 3G networks, and the buildout of giant server farms. All of this would make possible the technologies that are now the bedrock of the world's most powerful companies: algorithmic search, social media, mobile computing, cloud services, big-data analytics, AI, and more.

We think something similar is happening behind the wild volatility and stratospheric hype of the cryptocurrency and blockchain boom. The blockchain skeptics have crowed gleefully as crypto-token prices have tumbled from last year's dizzying highs, but they make the same mistake as the crypto fanboys they mock: they conflate price with inherent value. We can't yet predict what the blue-chip industries built on blockchain technology will be, but we are confident that they will exist, because the technology itself is all about creating one priceless asset: trust.

To understand why, we need to go back to the 14th century.

That was when Italian merchants and bankers began using the double-entry bookkeeping method. This method, made possible by the adoption of Arabic numerals, gave merchants a more reliable record-keeping tool, and it let bankers assume a powerful new role as middlemen in the international payments system. Yet it wasn't just the tool itself that made way for modern finance. It was how it was inserted into the culture of the day.

everything of value that merchants or bankers took in, they had to give something back. Hence the use of offsetting entries to record separate, balancing values—a debit matched with a credit, an asset with a liability.

Selman Design

Pacioli's morally upright accounting bestowed a form of religious benediction on these

We've allowed centralized trust managers such as banks, stock exchanges, and other financial middlemen to become indispensable, and this has turned them from intermediaries into gatekeepers. They charge fees and restrict access, creating friction, curtailing innovation, and strengthening their market dominance.

The real promise of blockchain technology, then, is not that it could make you a billionaire overnight or give you a way to shield your financial activities from nosy governments. It's that it could drastically reduce the cost of trust by means of a radical, decentralized approach to accounting—and, by extension, create a new way to structure economic organizations.

The need for trust and middlemen allows behemoths such as Google, Facebook, and Amazon to turn economies of scale and network effects into de facto monopolies.

A new form of bookkeeping might seem like a dull accomplishment. Yet for thousands of years, going back to Hammurabi's Babylon, ledgers have been the bedrock of civilization. That's because the exchanges of value on which society is founded require us to trust each other's claims about what we own, what we're owed, and what we owe. To achieve that trust, we need a common system for keeping track of our transactions, a system that gives definition and order to society itself. How else would we know that Jeff Bezos is the world's richest human being, that the GDP of Argentina is $620 billion, that 71 percent of the world's population lives on less than $10 a day, or that Apple's shares are trading at a particular multiple of the company's earnings per share?

A blockchain (though the term is bandied about loosely, and often misapplied to things that are not really blockchains) is an electronic ledger—a list of transactions. Those transactions can in principle represent almost anything. They could be actual exchanges of money, as they are on the blockchains that underlie cryptocurrencies like Bitcoin. They could mark exchanges of other assets, such as digital stock certificates. They could represent instructions, such as orders to buy or sell a stock. They could include so-called smart contracts, which are computerized instructions to do something (e.g., buy a stock) if something else is true (the price of the stock has dropped below $10).

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

automatically rejects the entry as invalid.

Related Story

Related Story

Half a billion dollars' worth of cryptocurrency was stolen—that's gotten people's attention.

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, for example, and often disagreements over which kind is most secure. 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-

same assets rendered the 158-year-old business bankrupt, triggering the biggest financial crisis in 80 years. Clearly, the valuations cited in the preceding years' books were way off. And we later learned that Lehman's ledger wasn't the only one with dubious data. Banks in the US and Europe paid out hundreds of billions of dollars in fines and settlements to cover losses caused by inflated balance sheets. It was a powerful reminder of the high price we often pay for trusting centralized entities' internally devised numbers.

Selman Design

Other manifestations of the cost of trust are felt not in what we do but in what we can't do. Two billion people are denied bank accounts, which locks them out of the global economy because banks don't trust the records of their assets and identities. Meanwhile, the internet of things, which it's hoped will have billions of interacting autonomous devices forging new efficiencies, won't be possible if gadget-to-gadget microtransactions require the prohibitively expensive intermediation of centrally controlled ledgers. There are many other examples of how this problem limits innovation.

These costs are rarely acknowledged or analyzed by the economics profession, perhaps because practices such as account reconciliation are assumed to be an integral, unavoidable feature of business (much as pre-internet businesses assumed they had no option but to pay large postal expenses to mail out monthly bills). Might this blind spot explain why some prominent economists are quick to dismiss blockchain technology? Many say they can't see the justification for its costs. Yet their analyses typically don't weigh those costs against the far-reaching societal cost of trust that the new models seek to overcome.

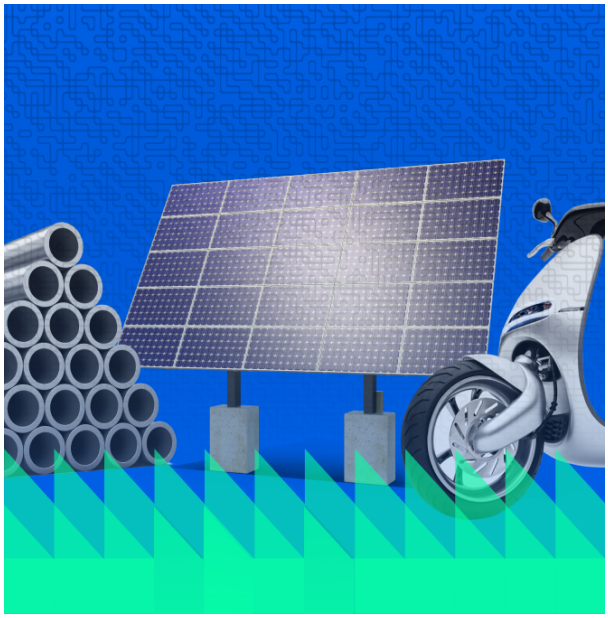
More and more people get it, however. Since Bitcoin's low-key release in January 2009, the ranks of its advocates have swelled from libertarian-minded radicals to include former Wall Street professionals, Silicon Valley tech mavens, and development and aid experts from bodies such as the World Bank. Many see the technology's rise as a vital new phase in the internet economy—one that is, arguably, even more transformative than the first. Whereas the first wave of online disruption saw brick-and-mortar businesses displaced by leaner digital intermediaries, this movement challenges the whole idea of for-profit middlemen altogether.

The need for trust, the cost of it, and the dependence on middlemen to provide it is one reason why behemoths such as Google, Facebook, and Amazon turn economies of scale and network-effect advantages into de facto monopolies. These giants are, in effect, centralized ledger keepers, building vast records of "transactions" in what is, arguably, the most important "currency" in the world: our digital data. In controlling those records, they control us.

The potential promise of overturning this entrenched, centralized system is an important factor behind the gold-rush-like scene in the crypto-token market, with its soaring yet volatile prices. No doubt many—perhaps most—investors are merely hoping to get rich quick and give little thought to why the technology matters. But manias like this, as irrational as they become, don't spring out of nowhere. As with the arrival of past transformative platform technologies—railroads, for example, or electricity—rampant speculation is almost inevitable. That's because when a big new idea comes along, investors have no framework for estimating how much value

Freely accessible open-source code is the foundation upon which the decentralized economy of the future will be built.

Companies such as IBM and Foxconn are exploiting the idea of immutability in projects that seek to unlock trade finance and make supply chains more transparent. Such transparency could also give consumers better information on the sources of what they buy—whether a T-shirt was made with sweatshop labor, for example.



Another important new idea is that of a *digital asset.* Before Bitcoin, nobody could own an asset in the digital realm. Since copying digital content is easy to do and difficult to stop, providers of digital products such as MP3 audio files or e-books never give customers outright ownership of the content, but instead lease it and define what users can do with it in a license, with stiff legal penalties if the license is broken. This is why you can make a 14-day loan of your Amazon Kindle book to a friend, but you can't sell it or give it as a gift, as you might a paper book.

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.

decentralized blockchain network. That assures all signatories to a smart contract that it will be carried out fairly.

With this technology, the computers of a shipper and an exporter, for example, could automate a transfer of ownership of goods once the decentralized software they both use sends a signal that a digital-currency payment—or a cryptographically unbreakable commitment to pay—has been made. Neither party necessarily trusts the other, but they can nonetheless carry out that automatic transfer without relying on a third party. In this way, smart contracts take automation to a new level—enabling a much more open, global set of relationships.

their self-interest and the common good. That was evident in many of the blockchain proposals from the 100 software engineers who took part in Hack4Climate at last year's UN climate-change conference in Bonn. The winning team, with a project called GainForest, is now developing a blockchain-based system by which donors can reward communities living in vulnerable rain forests for provable actions they take to restore the environment.

Still, this utopian, frictionless "token economy" is far from reality. Regulators in China, South Korea, and the US have cracked down on issuers and traders of tokens, viewing such currencies more as speculative get-rich-quick schemes that avoid securities laws than as world--changing new economic models. They're not entirely wrong: some developers have pre-sold tokens in "initial coin offerings," or ICOs, but haven't used the money to build and market products. Public or "permissionless" blockchains like Bitcoin and Ethereum, which hold the greatest promise of absolute openness and immutability, are facing growing pains. Bitcoin still can't process more than seven transactions a second, and transaction fees can sometimes spike, making it costly to use.

Related Story

Related Story

The ICO boom looks a lot like a bubble, but at its heart is a genuine innovation.

Meanwhile, the centralized institutions that should be vulnerable to disruption, such as banks, are digging in. They are protected by existing regulations, which are ostensibly imposed to keep them honest but inadvertently constitute a compliance cost for startups. Those regulations, such as the burdensome reporting and capital requirements that the New York State Department of Financial Services' "BitLicense" imposed on cryptocurrency remittance startups, become barriers to entry that protect incumbents.

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. It's reasonable to assume they will constantly improve the tech. Just as we've seen with internet software, open, extensible protocols such as these can become powerful platforms for innovation. Blockchain technology is moving way too fast for us to think later versions won't improve upon the present, whether it's in Bitcoin's cryptocurrency-based protocol, Ethereum's smart-contract-focused blockchain, or some as-yet-undiscovered platform.

The crypto bubble, like the dot-com bubble, is creating the infrastructure that will enable the technologies of the future to be built. But there's also a key difference. This time, the money being raised isn't underwriting *physical* infrastructure but *social* infrastructure. It's creating

platforms. Whether it's the open protocols of the internet or the blockchain's core components of algorithmic consensus and distributed record-keeping, their power lies in providing an entirely new paradigm for innovators ready to dream up and deploy world-changing applications. In this case, those applications—whatever shape they take—will be aimed squarely at disrupting many of the gatekeeping institutions that currently dominate our centralized economy.

by Michael J. Casey & Paul Vigna