McKinsey&Company

How blockchains could change the world

May 2016

Ignore Bitcoin's challenges. In this interview, Don Tapscott explains why blockchains, the technology underpinning the cryptocurrency, have the potential to revolutionize the world economy.

What impact could the technology behind Bitcoin have? According to Tapscott Group CEO Don Tapscott, blockchains, the technology underpinning the cryptocurrency, could revolutionize the world economy. In this interview with McKinsey's Rik Kirkland, Tapscott explains how blockchains—an open-source distributed database using state-of-the-art cryptography—may facilitate collaboration and tracking of all kinds of transactions and interactions. Tapscott, coauthor of the new book *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*, also believes the technology could offer genuine privacy protection and "a platform for truth and trust." An edited and extended transcript of Tapscott's comments follows.

Interview transcript

In the early 1990s, we said the old media is centralized. It's one way, it's one to many; it's controlled by powerful forces, and everyone is a passive recipient. The new web, the new media, we said, is one to one, it's many to many; it's highly distributed, and it's not centralized. Everyone's a participant, not an inert recipient. This has an awesome neutrality. It will be what we want it to be, and we can craft a much more egalitarian, prosperous society where everyone gets to share in the wealth that they create. Lots of great things have happened, but overall the benefits of the digital age have been asymmetrical. For example, we have this great asset of data that's been created by us, and yet we don't get to keep it. It's owned by a tiny handful of powerful companies or governments. They monetize that data or, in the case of governments, use it to spy on us, and our privacy is undermined.

What if there were a second generation of the Internet that enabled the true, peer-to-peer exchange of value? We don't have that now. If I'm going to send some money to somebody else, I have to go through an intermediary—a powerful bank, a credit-card company—or I need

a government to authenticate who I am and who you are. What if we could do that peer to peer? What if there was a protocol—call it the trust protocol—that enabled us to do transactions, to do commerce, to exchange money, without a powerful third party? This would be amazing.

Several years ago, an unknown person or persons named Satoshi Nakamoto came up with the Bitcoin protocol. Once again, the technology genie has been unleashed from its bottle. It gives us another kick at the can, another go, to try and rethink the economic power grid and the old order of things. That, to me, is how big this is. It feels like 1993.

How the blockchain works

The blockchain is basically a distributed database. Think of a giant, global spreadsheet that runs on millions and millions of computers. It's distributed. It's open source, so anyone can change the underlying code, and they can see what's going on. It's truly peer to peer; it doesn't require powerful intermediaries to authenticate or to settle transactions.

It uses state-of-the-art cryptography, so if we have a global, distributed database that can record the fact that we've done this transaction, what else could it record? Well, it could record any structured information, not just who paid whom but also who married whom or who owns what land or what light bought power from what power source. In the case of the Internet of Things, we're going to need a blockchain-settlement system underneath. Banks won't be able to settle trillions of real-time transactions between things.

So this is an extraordinary thing. An immutable, unhackable distributed database of digital assets. This is a platform for truth and it's a platform for trust. The implications are staggering, not just for the financial-services industry but also right across virtually every aspect of society.

Most blockchains—and Bitcoin is the biggest—are what you call permission-less systems. We can do transactions and satisfy each other's economic needs without knowing who the other party is and independent from central authorities. These blockchains all have a digital currency of some kind associated with them, which is why everybody talks about Bitcoin in the same breath as the blockchain, because the Bitcoin blockchain is the biggest.

But to me, the blockchain, the underlying technology, is the biggest innovation in computer science—the idea of a distributed database where trust is established through mass collaboration and clever code rather than through a powerful institution that does the authentication and the settlement.

The way it works is, if I owe you $20, we do the transaction. There's a huge community called miners, and they have a powerful computing resource. Some people have estimated that the entire computing power of Google would be 5 percent of this blockchain-computing power, for the Bitcoin blockchain. That platform solves this big, big problem called the double-payment problem. If I send you an MP3 file and I send it to somebody else, it's a problem for the record industry, but it's not a massive problem. If I send you $20, and I send the same file to somebody else, that's a big problem. It's called fraud, and the economy stops if you have a monetary

system based on that. What happens is, I send you the $20, and these miners, to make a long story short, go about authenticating that the transaction occurred.

Each miner is motivated to be the first one to find the truth, and once you find the truth, it's evidence to everybody else. When you find the truth and you solve a complex mathematical problem, you get paid some money, some Bitcoin. For me to hack that and try and send the same money to somebody else, or for me to come in and try and take your $20 worth of Bitcoins, is not practically possible because I'd have to hack that ten-minute block. That's why it's called blockchain, and that block is linked to the previous block, and the previous block—ergo, chain. This blockchain is running across countless numbers of computers. I would have to commit fraud in the light of the most powerful computing resource in the world, not just for that ten-minute block but for the entire history of commerce, on a distributed platform. This is not practically feasible.

So, sure, there have been lots of problems with Bitcoin. You had big exchanges like Mt. Gox fail. You had the Silk Road, where Bitcoin was the payment system for all kinds of horrific, illegal activity. But don't be confused by that. Many people make the mistake of thinking, "Bitcoin? Well, that's an asset. Should I invest? Is it going to go up or down?" Well, that's not of interest to me, just like speculating in gold is not of interest to me.

Something that's of bigger interest is Bitcoin as a digital currency that enables us to do these kinds of transactions. A cryptocurrency that's not based on nation-states. The most important thing that we focus on in our work, is the much bigger question, this underlying, distributed-database technology that enables us to have a truthful and immutable record of everything.

How disruption can occur

The financial-services industry is up for serious disruption—or transformation, depending on how it approaches this issue. For the research for *Blockchain Revolution*, we went through and identified eight different things that the industry does: it moves money, it stores money, it lends money, it trades money, it attests to money, it accounts for money, and so on.

Every one of those can be challenged.

You pick any industry, and this technology holds huge potential to disrupt it, creating a more prosperous world where people get to participate in the value that they create. The music industry, for example, is a disaster, at least from the point of view of the musicians. They used to have most of the value taken by the big labels. Then, along came the technology companies, which took a whole bunch of value, and the songwriters and musicians are left with crumbs at the end. What if the new music industry was a distributed app on the blockchain, where I, as a songwriter, could post my song onto the blockchain with a smart contract specifying how it is to be used?

Maybe as a recording artist posting my music on a blockchain music platform, I'll say, "You listen to the music, it's free. You want to put it in your movie? It's going to cost you this much,

and here's how that works. You put it in the movie, the smart contract pays me." Or how about using it for a ring tone? There's the smart contract for that.

This is not a pipe dream. Imogen Heap, who's a brilliant singer-songwriter in the United Kingdom, a best-selling recording artist, has now been part of creating Mycelia, and they're working with an amazing company called Consensus Systems, that's all around the world, blockchain developers, using the Ethereum platform; Ethereum is one blockchain. She has already posted her first song onto the Internet. I fully expect that many big recording artists will be seriously investigating a whole new paradigm whereby the musicians get compensated for the value that they create.

What could go wrong?

I'm not a futurist. I think the future's not something to be predicted—it's something to be achieved. What we're arguing is that this technology is revolutionary and holds vast potential to change society.

What could go wrong? We identified ten showstoppers and we went through them in detail in our research and in the book. There are showstoppers such as the energy that's consumed to do this, which is massive. Another showstopper is that this technology is going to be the platform for a lot of smart agents that are going to displace a lot of humans from jobs. Maybe this whole new platform is the ultimate job-killer.

The biggest problems, though, have to do with governance. Any controversy that you read about today is going to revolve around these governance issues. This new community is in its infancy. Unlike the Internet, which has a sophisticated governance ecosystem, the whole world of blockchain and digital currencies is the Wild West.

It's a place of recklessness and chaos and calamity. This could kill it if we don't find the leadership to come together and to create the equivalent organizations that we have for governance of the Internet. We have the Internet Engineering Task Force, which creates standards for the Net. We have Internet Governance Forum, which creates policies for governments. We have the W3C Consortium, which creates standards for the Web. There's the Internet Society; that's an advocacy group. There's the Internet Corporation for Assigned Names and Numbers (ICANN), an operational network that just delivers the domain names. There's a structure and a process to figure out things. Right now, there's a big debate that continues about the block size. We need a bigger block size to be able to handle all of the transactions that will be arising. There are big differences. There are legitimate points of view, but the problem is, there's no process to be able to come up with an optimal solution.

I'm hopeful, even optimistic, that this will proceed. It feels a lot like the early '90s to me. You've got all the smartest venture capitalists, the smartest programmers, the smartest business executives, the smartest people in banking, the smartest government of people, the smartest

entrepreneurs all over this thing. That's always a sign that something big is going on. Is it an irrational exuberance? I don't know. Last year, $1 billion went into venture alone in this area. I'm more hopeful because I can see the power of the applications to disrupt things for the good. Rather than just redistributing wealth, maybe we could change the way wealth is distributed in the first place. Imagine a Kickstarter-like campaign to launch a company where you have 50 million investors and everybody puts in a couple of dollars, or very small amounts.

Imagine all those people who have a supercomputer in their pocket, who are connected to a network but don't have a bank account, because they only own a couple of pigs and a chicken. That's their bank account. Imagine if they could be brought in, 2 billion people, into the global financial system. What could that do? Seventy percent of all people who own land have a tenuous title to that land. And you're in a developing-world country in Latin America, and some dictator comes to power and he says, "Well, you may have a piece of paper that says you own your little farm, but my central computer says my friend owns your farm."

Imagine a world where foreign aid didn't get consumed in the bureaucracy but went directly to the beneficiary under a smart contract? Rather than a $60 billion car-service aggregation, why couldn't we have a distributed app on the blockchain that manages all these vehicles and handles everything from reputation to payments? Ultimately, they'll be autonomous vehicles moving around. Or blockchain Airbnb? This is all about the value going to the creators of value rather than to powerful forces that capture it. In the process, we can protect our privacy. Privacy is a basic human right, and people who say "It's dead—get over it" are deeply misinformed. It's the foundation of a free society.

Imagine each of us having our own identity in a black box on the blockchain. When you go to do a transaction, it gives away a shred of information required to do that transaction and it collects data. You get to keep your data and monetize it if you want, or not. This could be the foundation of a whole new era whereby our basic right to privacy is protected, because identity is the foundation of freedom and it needs to be managed responsibly.

We've been unable to do that, so far. I'm compelled most by the power of this opportunity. I've been at this 35 years, writing about the digital age. I've never seen a technology that I thought had greater potential for humanity. □

For more about *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*, visit penguinrandomhouse.com.

Don Tapscott, CEO of the Tapscott Group, is coauthor, with his son, **Alex,** of *Blockchain Revolution*. **Rik Kirkland** is the senior managing editor of McKinsey Publishing and is based in McKinsey's New York office.