Harvard Business Review

TECHNOLOGY

The Truth About Blockchain

by Marco Iansiti and Karim R. Lakhani

FROM THE JANUARY–FEBRUARY 2017 ISSUE

Contracts, transactions, and the records of them are among the defining structures in our economic, legal, and political systems. They protect assets and set organizational boundaries. They establish and verify identities and chronicle events. They govern interactions among nations, organizations, communities, and individuals. They guide managerial and social action. And yet these critical tools and the bureaucracies formed to manage them have not kept up with the economy's digital transformation. They're like a rush-hour gridlock trapping a Formula 1 race car. In a digital world, the way we regulate and maintain administrative control has to change.

Blockchain promises to solve this problem. The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically.

How Blockchain Works

Here are five basic principles underlying the technology.

1. Distributed Database

With blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. In this world every agreement, every process, every task, and

Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

2. Peer-to-Peer Transmission
Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes.

3. Transparency with Pseudonymity
Every transaction and its associated value are visible to anyone with access to the system. Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.

4. Irreversibility of Records
Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, because they're linked to every transaction record that came before them (hence the term "chain"). Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.

every payment would have a digital record and signature that could be identified, validated, stored, and shared. Intermediaries like lawyers, brokers, and bankers might no longer be necessary. Individuals, organizations, machines, and algorithms would freely transact and interact with one another with little friction. This is the immense potential of blockchain.

Indeed, virtually everyone has heard the claim that blockchain will revolutionize business and redefine companies and economies. Although we share the enthusiasm for its potential, we worry about the hype. It's not just security issues (such as the 2014 collapse of one bitcoin exchange and the more recent hacks of others) that concern us. Our experience studying technological innovation tells us that if there's to be a blockchain revolution, many barriers—technological, governance, organizational, and even societal—will have to fall. It would be a mistake to rush headlong into blockchain innovation without understanding how it is likely to take hold.

True blockchain-led transformation of business and government, we believe, is still many years away. That's because blockchain

5. Computational Logic
The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. So users can set up algorithms and rules that automatically trigger transactions between nodes.

is not a "disruptive" technology, which can attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly. Blockchain is a *foundational* technology: It has the potential to create new foundations for our economic and social systems. But while the impact will be enormous, it will take decades for blockchain to seep into our economic and social infrastructure. The process of adoption will be gradual and steady, not sudden, as waves of technological and institutional change gain momentum. That insight and its strategic implications are what we'll explore in this article.

Patterns of Technology Adoption

Before jumping into blockchain strategy and investment, let's reflect on what we know about technology adoption and, in particular, the transformation process typical of other foundational technologies. One of the most relevant examples is distributed computer networking technology, seen in the adoption of TCP/IP (transmission control protocol/internet protocol), which laid the groundwork for the development of the internet.

Introduced in 1972, TCP/IP first gained traction in a *single-use* case: as the basis for e-mail among the researchers on ARPAnet, the U.S. Department of Defense precursor to the commercial internet. Before TCP/IP, telecommunications architecture was based on "circuit switching," in which connections between two parties or machines had to be preestablished and sustained throughout an exchange. To ensure that any two nodes could communicate, telecom service providers and equipment manufacturers had invested billions in building dedicated lines.

TCP/IP turned that model on its head. The new protocol transmitted information by digitizing it and breaking it up into very small packets, each including address information. Once released into the network, the packets could take any route to the recipient. Smart sending and receiving nodes at the network's edges could disassemble and reassemble the packets and interpret the encoded data. There was no need for dedicated private lines or massive infrastructure. TCP/IP created an open, shared public network without any central authority or party responsible for its maintenance and improvement.

Traditional telecommunications and computing sectors looked on TCP/IP with skepticism. Few imagined that robust data, messaging, voice, and video connections could be established on the new architecture or that the associated system could be secure and scale up. But during the late 1980s and 1990s, a growing number of firms, such as Sun, NeXT, Hewlett-Packard, and Silicon Graphics, used TCP/IP, in part to create *localized* private networks within organizations. To do so, they developed building blocks and tools that broadened its use beyond e-mail, gradually replacing more-traditional local network technologies and standards. As organizations adopted these building blocks and tools, they saw dramatic gains in productivity.

TCP/IP burst into broad public use with the advent of the World Wide Web in the mid-1990s. New technology companies quickly emerged to provide the "plumbing"—the hardware, software, and services needed to connect to the now-public network and exchange information. Netscape commercialized browsers, web servers, and other tools and components that aided the development and adoption of internet services and applications. Sun drove the development of Java, the application-programming language. As information on the web grew exponentially, Infoseek, Excite, AltaVista, and Yahoo were born to guide users around it.

Once this basic infrastructure gained critical mass, a new generation of companies took advantage of low-cost connectivity by creating internet services that were compelling *substitutes* for existing businesses. CNET moved news online. Amazon offered more books

for sale than any bookshop. Priceline and Expedia made it easier to buy airline tickets and brought unprecedented transparency to the process. The ability of these newcomers to get extensive reach at relatively low cost put significant pressure on traditional businesses like newspapers and brick-and-mortar retailers.

Relying on broad internet connectivity, the next wave of companies created novel, *transformative* applications that fundamentally changed the way businesses created and captured value. These companies were built on a new peer-to-peer architecture and generated value by coordinating distributed networks of users. Think of how eBay changed online retail through auctions, Napster changed the music industry, Skype changed telecommunications, and Google, which exploited user-generated links to provide more relevant results, changed web search.

> Companies are already using blockchain to track items through complex supply chains.

Ultimately, it took more than 30 years for TCP/IP to move through all the phases—single use, localized use, substitution, and transformation—and reshape the economy. Today more than half the world's most valuable public companies have internet-driven, platform-based business models. The very foundations of our economy have changed. Physical scale and unique intellectual property no longer confer unbeatable advantages; increasingly, the economic leaders are enterprises that act as "keystones," proactively organizing, influencing, and coordinating widespread networks of communities, users, and organizations.

The New Architecture

Blockchain—a peer-to-peer network that sits on top of the internet—was introduced in October 2008 as part of a proposal for bitcoin, a virtual currency system that eschewed a central authority for issuing currency, transferring ownership, and confirming transactions.

Bitcoin is the first application of blockchain technology.

The parallels between blockchain and TCP/IP are clear. Just as e-mail enabled bilateral messaging, bitcoin enables bilateral financial transactions. The development and maintenance of blockchain is open, distributed, and shared—just like TCP/IP's. A team of volunteers around the world maintains the core software. And just like e-mail, bitcoin first caught on with an enthusiastic but relatively small community.

TCP/IP unlocked new economic value by dramatically lowering the cost of connections. Similarly, blockchain could dramatically reduce the cost of transactions. It has the potential to become the system of record for all transactions. If that happens, the economy will once again undergo a radical shift, as new, blockchain-based sources of influence and control emerge.

Consider how business works now. Keeping ongoing records of transactions is a core function of any business. Those records track past actions and performance and guide planning for the future. They provide a view not only of how the organization works internally but also of the organization's outside relationships. Every organization keeps its own records, and they're private. Many organizations have no master ledger of all their activities; instead records are distributed across internal units and functions. The problem is, reconciling transactions across individual and private ledgers takes a lot of time and is prone to error.

For example, a typical stock transaction can be executed within microseconds, often without human intervention. However, the settlement—the ownership transfer of the stock—can take as long as a week. That's because the parties have no access to each other's ledgers and can't automatically verify that the assets are in fact owned and can be transferred. Instead a series of intermediaries act as guarantors of assets as the record of the transaction traverses organizations and the ledgers are individually updated.

In a blockchain system, the ledger is replicated in a large number of identical databases, each hosted and maintained by an interested party. When changes are entered in one copy, all the other copies are simultaneously updated. So as transactions occur, records of the value and assets exchanged are permanently entered in all ledgers. There is no need for third-party intermediaries to verify or transfer ownership. If a stock transaction took place on a blockchain-based system, it would be settled within seconds, securely and verifiably. (The infamous hacks that have hit bitcoin exchanges exposed weaknesses not in the blockchain itself but in separate systems linked to parties using the blockchain.)

A Framework for Blockchain Adoption

If bitcoin is like early e-mail, is blockchain decades from reaching its full potential? In our view the answer is a qualified yes. We can't predict exactly how many years the transformation will take, but we can guess which kinds of applications will gain traction first and how blockchain's broad acceptance will eventually come about.

How Foundational Technologies Take Hold

The adoption of foundational technologies typically happens in four phases. Each phase is defined by the novelty of the applications and the complexity of the coordination efforts needed to make them workable. Applications low in novelty and complexity gain acceptance first. Applications high in novelty and complexity take decades to evolve but can transform the economy. TCP/IP technology, introduced on ARPAnet in 1972, has already reached the

In our analysis, history suggests that two dimensions affect how a foundational technology and its business use cases evolve. The first is novelty—the degree to which an application is new to the world. The more novel it is, the more effort will be required to ensure that users understand what problems it solves. The second dimension is complexity, represented by the level of ecosystem coordination involved—the number and diversity of parties that need to work together to produce value with the technology. For example, a social network with just one member is of little use; a social network is worthwhile only when many of

transformation phase, but blockchain applications (in red) are in their early days.

your own connections have signed on to it. Other users of the application must be brought on board to generate value for all participants. The same will be true for many blockchain applications. And, as the scale and impact of those applications increase, their adoption will require significant institutional change.

We've developed a framework that maps innovations against these two contextual dimensions, dividing them into quadrants. (See the exhibit "How Foundational Technologies Take Hold.") Each quadrant represents a stage of technology development. Identifying which one a blockchain innovation falls into will help executives understand the types of challenges it presents, the level of collaboration and consensus it needs, and the legislative and regulatory efforts it will require. The map will also suggest what kind of processes and infrastructure must be established to facilitate the innovation's adoption. Managers can use it to assess the state of blockchain development in any industry, as well as to evaluate strategic investments in their own blockchain capabilities.

Single use.

In the first quadrant are low-novelty and low-coordination applications that create better, less costly, highly focused solutions. E-mail, a cheap alternative to phone calls, faxes, and snail mail, was a single-use application for TCP/IP (even though its value rose with the number of users). Bitcoin, too, falls into this quadrant. Even in its early days, bitcoin offered immediate value to the few people who used it simply as an alternative payment method. (You can think of it as a complex e-mail that transfers not just information but also actual value.) At the end of 2016 the value of bitcoin transactions was expected to hit $92 billion. That's still a rounding error compared with the $411 trillion in total global payments, but bitcoin is growing fast and increasingly important in contexts such as instant payments and foreign currency and asset trading, where the present financial system has limitations.

Localization.

The second quadrant comprises innovations that are relatively high in novelty but need only a limited number of users to create immediate value, so it's still relatively easy to promote their adoption. If blockchain follows the path network technologies took in business, we can expect blockchain innovations to build on single-use applications to create local private networks on which multiple organizations are connected through a distributed ledger.

Much of the initial private blockchain-based development is taking place in the financial services sector, often within small networks of firms, so the coordination requirements are relatively modest. Nasdaq is working with Chain.com, one of many blockchain infrastructure providers, to offer technology for processing and validating financial transactions. Bank of America, JPMorgan, the New York Stock Exchange, Fidelity Investments, and Standard Chartered are testing blockchain technology as a replacement for paper-based and manual transaction processing in such areas as trade finance, foreign exchange, cross-border settlement, and securities settlement. The Bank of Canada is testing a digital currency called CAD-coin for interbank transfers. We anticipate a proliferation of private blockchains that serve specific purposes for various industries.

Substitution.

The third quadrant contains applications that are relatively low in novelty because they build on existing single-use and localized applications, but are high in coordination needs because they involve broader and increasingly public uses. These innovations aim to replace entire ways of doing business. They face high barriers to adoption, however; not only do they require more coordination but the processes they hope to replace may be full-blown and deeply embedded within organizations and institutions. Examples of substitutes include cryptocurrencies—new, fully formed currency systems that have grown out of the simple bitcoin payment technology. The critical difference is that a cryptocurrency requires every party that does monetary transactions to adopt it, challenging governments and

institutions that have long handled and overseen such transactions. Consumers also have to change their behavior and understand how to implement the new functional capability of the cryptocurrency.

A recent experiment at MIT highlights the challenges ahead for digital currency systems. In 2014 the MIT Bitcoin Club provided each of MIT's 4,494 undergraduates with $100 in bitcoin. Interestingly, 30% of the students did not even sign up for the free money, and 20% of the sign-ups converted the bitcoin to cash within a few weeks. Even the technically savvy had a tough time understanding how or where to use bitcoin.

One of the most ambitious substitute blockchain applications is Stellar, a nonprofit that aims to bring affordable financial services, including banking, micropayments, and remittances, to people who've never had access to them. Stellar offers its own virtual currency, lumens, and also allows users to retain on its system a range of assets, including other currencies, telephone minutes, and data credits. Stellar initially focused on Africa, particularly Nigeria, the largest economy there. It has seen significant adoption among its target population and proved its cost-effectiveness. But its future is by no means certain, because the ecosystem coordination challenges are high. Although grassroots adoption has demonstrated the viability of Stellar, to become a banking standard, it will need to influence government policy and persuade central banks and large organizations to use it. That could take years of concerted effort.

Further Reading

To learn more about technology adoption, go to these articles on HBR.org:

"Digital Ubiquity: How Connections, Sensors, and Data Are Revolutionizing Business"
Marco Iansiti and Karim R. Lakhani

Transformation.

Into the last quadrant fall completely novel applications that, if successful, could change the very nature of economic, social, and political systems. They involve coordinating the activity of many actors and gaining

"Strategy as Ecology"
Marco Iansiti and Roy Levien

"Right Tech, Wrong Time"
Ron Adner and Rahul Kapoor

institutional agreement on standards and processes. Their adoption will require major social, legal, and political change.

"Smart contracts" may be the most transformative blockchain application at the moment. These automate payments and the transfer of currency or other assets as negotiated conditions are met. For example, a smart contract might send a payment to a supplier as soon as a shipment is delivered. A firm could signal via blockchain that a particular good has been received—or the product could have GPS functionality, which would automatically log a location update that, in turn, triggered a payment. We've already seen a few early experiments with such self-executing contracts in the areas of venture funding, banking, and digital rights management.

The implications are fascinating. Firms are built on contracts, from incorporation to buyer-supplier relationships to employee relations. If contracts are automated, then what will happen to traditional firm structures, processes, and intermediaries like lawyers and accountants? And what about managers? Their roles would all radically change. Before we get too excited here, though, let's remember that we are decades away from the widespread adoption of smart contracts. They cannot be effective, for instance, without institutional buy-in. A tremendous degree of coordination and clarity on how smart contracts are designed, verified, implemented, and enforced will be required. We believe the institutions responsible for those daunting tasks will take a long time to evolve. And the technology challenges—especially security—are daunting.

Guiding Your Approach to Blockchain Investment

How should executives think about blockchain for their own organizations? Our framework can help companies identify the right opportunities.

For most, the easiest place to start is single-use applications, which minimize risk because they aren't new and involve little coordination with third parties. One strategy is to add bitcoin as a payment mechanism. The infrastructure and market for bitcoin are already well developed, and adopting the virtual currency will force a variety of functions, including IT, finance, accounting, sales, and marketing, to build blockchain capabilities. Another low-risk approach is to use blockchain internally as a database for applications like managing physical and digital assets, recording internal transactions, and verifying identities. This may be an especially useful solution for companies struggling to reconcile multiple internal databases. Testing out single-use applications will help organizations develop the skills they need for more-advanced applications. And thanks to the emergence of cloud-based blockchain services from both start-ups and large platforms like Amazon and Microsoft, experimentation is getting easier all the time.

Localized applications are a natural next step for companies. We're seeing a lot of investment in private blockchain networks right now, and the projects involved seem poised for real short-term impact. Financial services companies, for example, are finding that the private blockchain networks they've set up with a limited number of trusted counterparties can significantly reduce transaction costs.

Organizations can also tackle specific problems in transactions across boundaries with localized applications. Companies are already using blockchain to track items through complex supply chains, for instance. This is happening in the diamond industry, where gems are being traced from mines to consumers. The technology for such experiments is now available off-the-shelf.

Developing substitute applications requires careful planning, since existing solutions may be difficult to dislodge. One way to go may be to focus on replacements that won't require end users to change their behavior much but present alternatives to expensive or unattractive solutions. To get traction, substitutes must deliver functionality as good as a traditional solution's and must be easy for the ecosystem to absorb and adopt. First Data's

foray into blockchain-based gift cards is a good example of a well-considered substitute. Retailers that offer them to consumers can dramatically lower costs per transaction and enhance security by using blockchain to track the flows of currency within accounts—without relying on external payment processors. These new gift cards even allow transfers of balances and transaction capability between merchants via the common ledger.

> Blockchain could slash the cost of transactions and reshape the economy.

Transformative applications are still far away. But it makes sense to evaluate their possibilities now and invest in developing technology that can enable them. They will be most powerful when tied to a new business model in which the logic of value creation and capture departs from existing approaches. Such business models are hard to adopt but can unlock future growth for companies.

Consider how law firms will have to change to make smart contracts viable. They'll need to develop new expertise in software and blockchain programming. They'll probably also have to rethink their hourly payment model and entertain the idea of charging transaction or hosting fees for contracts, to name just two possible approaches. Whatever tack they take, executives must be sure they understand and have tested the business model implications before making any switch.

Transformative scenarios will take off last, but they will also deliver enormous value. Two areas where they could have a profound impact: large-scale public identity systems for such functions as passport control, and algorithm-driven decision making in the prevention of money laundering and in complex financial transactions that involve many parties. We expect these applications won't reach broad adoption and critical mass for at least another decade and probably more.

Transformative applications will also give rise to new platform-level players that will coordinate and govern the new ecosystems. These will be the Googles and Facebooks of the next generation. It will require patience to realize such opportunities. Though it may be premature to start making significant investments in them now, developing the required foundations for them—tools and standards—is still worthwhile.

CONCLUSION

In addition to providing a good template for blockchain's adoption, TCP/IP has most likely smoothed the way for it. TCP/IP has become ubiquitous, and blockchain applications are being built on top of the digital data, communication, and computation infrastructure, which lowers the cost of experimentation and will allow new use cases to emerge rapidly.

With our framework, executives can figure out where to start building their organizational capabilities for blockchain today. They need to ensure that their staffs learn about blockchain, to develop company-specific applications across the quadrants we've identified, and to invest in blockchain infrastructure.

But given the time horizons, barriers to adoption, and sheer complexity involved in getting to TCP/IP levels of acceptance, executives should think carefully about the risks involved in experimenting with blockchain. Clearly, starting small is a good way to develop the know-how to think bigger. But the level of investment should depend on the context of the company and the industry. Financial services companies are already well down the road to blockchain adoption. Manufacturing is not.

No matter what the context, there's a strong possibility that blockchain will affect your business. The very big question is when.

A version of this article appeared in the January–February 2017 issue (pp.118–127) of *Harvard Business Review*.

Marco Iansiti is the David Sarnoff Professor of Business Administration at Harvard Business School in Boston. Twitter: @marcoiansiti and @digHBS

Karim R. Lakhani is the Lumry Family Associate Professor of Business Administration at the Harvard Business School and the Principal Investigator of the Harvard-NASA Tournament Lab at the Institute for Quantitative Social Science. Follow him on Twitter @klakhani

This article is about TECHNOLOGY

⊕ **FOLLOW** THIS TOPIC

Comments

Leave a Comment

POST

6 COMMENTS

Ville Viitasaari 4 days ago

I must say this was a pleasure to read. The long-term possibilities were presented without hype. However, I believe the coming transformation may be faster this time. The open-source community is thriving and, since blockchain / distributive ledger tech is essentially open-source, development cycles are short. What I think could be major game changers in the short-term (a few years) are blockchain based digital fiat currencies i.e. "sovereign blockchains". The benefits to society are simply too big for central banks to look the other way. And then we could invest saved transaction fees in cheap solar panels and build "neighborhood solar panel networks" to trade local electricity -- all in the sovereign blockchain.

REPLY

0 0

JOIN THE CONVERSATION

POSTING GUIDELINES

We hope the conversations that take place on HBR.org will be energetic, constructive, and thought-provoking. To comment, readers must sign in or register. And to ensure the quality of the discussion, our moderating team will review all comments and may edit them for clarity, length, and relevance. Comments that are overly promotional, mean-spirited, or off-topic may be deleted per the moderators' judgment. All postings become the property of Harvard Business Publishing.