strategy+business

ISSUE 82 SPRING 2016

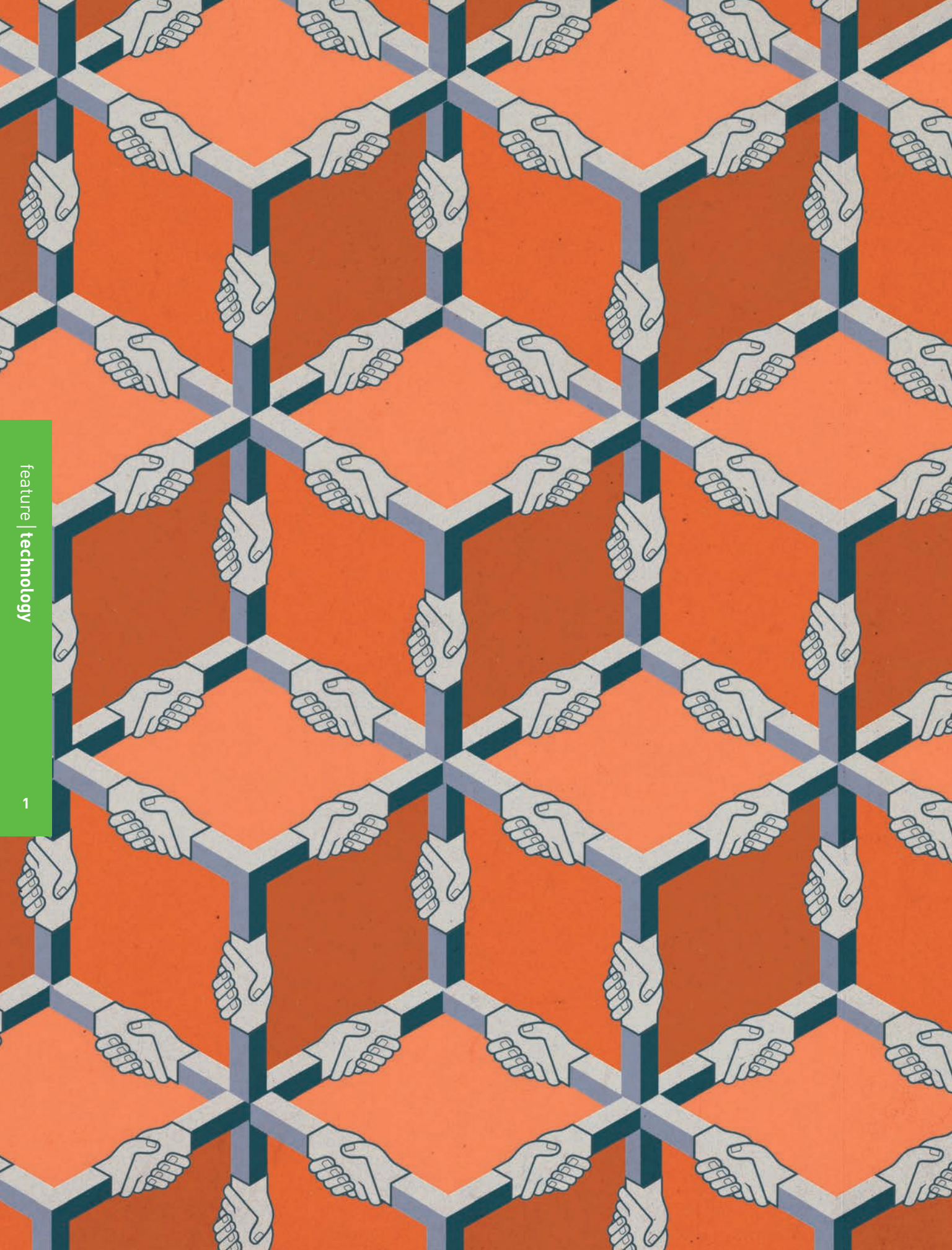
A Strategist's Guide to Blockchain

The distributed ledger technology that started with bitcoin is rapidly becoming a crowdsourced system for all types of verification. Could it replace notary publics, manual vote recounts, and the way banks manage transactions?

BY JOHN PLANSKY, TIM O'DONNELL, AND KIMBERLY RICHARDS

REPRINT 16111

pwc | strategy&



A STRATEGIST'S GUIDE TO BLOCKCHAIN

The distributed ledger technology that started with bitcoin is rapidly becoming a crowdsourced system for all types of verification. Could it replace notary publics, manual vote recounts, and the way banks manage transactions?

BY JOHN PLANSKY, TIM O'DONNELL, AND KIMBERLY RICHARDS

An expensive work of art changes hands. Neither the buyer nor the seller is named publicly, but the exchange is verified, the provenance of the painting travels with it, and the artwork is automatically insured against theft.

A voting machine records votes in a frontier country known for past political corruption. Though there is no central government repository, each vote is tagged to an individual with no duplication. The individual identities remain anonymous, and the results of the election are undisputed.

Illustration by Dan Page

John Plansky
john.plansky@strategyand.us.pwc.com
is an advisor to executives in the financial-services industry for Strategy&, PwC's strategy consulting group. Based in Boston, he is a principal with PwC US. He specializes in applying information technology to launch new products and enable global operating models for securities firms.

Tim O'Donnell
timothy.b.odonnell@us.pwc.com
is a managing director with PwC US based in New York, specializing in banking products and operations strategies. He has extensive experience with payments innovation and technology solutions.

Kimberly Richards
kimberly.richards@strategyand.us.pwc.com
is a specialist in financial-services strategy with Strategy&. She is a manager with PwC US based in New York.

Also contributing to this article were PwC US director Jeremy Drane, principal Kevin Grieve, managing director James Solomon, Technology Institute editor Alan Morrison, and Financial Services Institute director Cathryn Marsh.

A consortium of banks gain market share by settling trades in real time (instead of waiting three days for the trade to clear) and underwriting loans in a day (instead of waiting two weeks), all with minimal risk. The same banks also start to execute same-day currency trades at optimal exchange rates, spending a fraction of the costs required in the past. All of these transactions are tracked and statistics are kept, so that governments are aware of the movement of capital across their borders, and activity is monitored for patterns that might indicate money laundering. But the identity of the individual traders or purchasers is untraceable.

The technology that could make all this happen is blockchain. Originally the formal name of the tracking database underlying the digital currency bitcoin, the term is now used broadly to refer to any distributed electronic ledger that uses software algorithms to record transactions with reliability and anonymity. This technology is also sometimes referred to as *distributed ledgers* (its more generic name), *cryptocurrencies* (the electronic currencies that first engendered it), *bitcoin* (the most prominent of those cryptocurrencies), and *decentralized verification* (the key differentiating attribute of this type of system).

At its heart, blockchain is a self-sustaining, peer-to-peer database technology for managing and recording transactions with no central bank or clearinghouse involvement. Because blockchain verification is handled through algorithms and consensus among multiple computers, the system is presumed immune to tampering, fraud, or political control. It is designed to protect against domination of the network by any single computer or group of computers. Participants are relatively anonymous, identified only by pseudonyms, and every transaction can be relied upon. Moreover, because every core transaction is processed just once, in one shared electronic ledger, blockchain reduces the redundancy and delays that exist in today's banking system.

Companies expressing interest in blockchain include HP, Microsoft, IBM, and Intel. In the financial-services sector, some large firms are forging partnerships with technology-focused startups to explore their own possibilities. For example, R3, a financial technology firm, announced in October 2015 that 25 banks had joined its consortium, which is attempting to develop a common crypto-technology-based platform. Participants include such influential banks as Citi, Bank of America, HSBC, Deutsche Bank, Morgan Stanley, UniCredit, Société Générale, Mitsubishi UFG Financial Group, National Australia Bank, and the Royal Bank of Canada. Another early experimenter is Nasdaq, whose CEO, Robert Greifeld, introduced Nasdaq Linq, a blockchain-based digital ledger for transferring shares of privately held companies, also in October 2015.

If experiments like these pan out, blockchain technology could become a game-changing force in any venue where trading occurs, where trust is at a premium, and where people need protection from identity theft — including the public sector (managing public records and elections), healthcare (keeping records anonymous but easily available), retail (handling large-ticket purchases such as auto leasing and real estate), and, of course, all forms of financial services. Indeed, some farsighted banks are already exploring how blockchain might transform their approaches to trading and settling, back-office operations, and investment and capital assets management. They recognize that the technology could become a differentiating factor in their own

Blockchain could affect transactions in the same way that GPS changed personal transportation.

capabilities, enabling them to process transactions with more efficiency, security, privacy, reliability, and speed. It is possible that blockchain could affect transactions in the same way that the global positioning system (GPS) changed personal transportation, by making data accessible through a common electronic platform.

But although the potential is immense, so is the uncertainty. On the one hand, distributed ledger technologies are so new, so complex, and so evolving so rapidly that it's difficult to predict what form they will ultimately take — or even to be sure they will work. The Gartner Group declared in an August 2015 report that cryptocurrency was traveling a "hype cycle": It had passed the Peak of Inflated Expectations and was headed for the Trough of Disillusionment. Another research firm, Forrester, titled its 2015 blockchain report "Don't Believe in Miracles," advising enterprises to wait five to 10 years before introducing blockchain, in part because of legal restrictions.

On the other hand, some authorities advocate energetic R&D. "The distributed payment technology embodied in bitcoin has real potential," said Andrew Haldane, chief economist of the Bank of England, in September 2015. "On the face of it, it solves a deep problem in monetary economics: how to establish trust — the essence of money — in a distributed network."

Strategists take note: Proceed deliberately. Don't try to convert existing systems to blockchain initiatives right away. Rather, explore how others might try to disrupt your business with distributed ledger technology, and how your company could use it to leap ahead instead. Put one or two pilot projects into place. In all cases, link your investments to your value proposition, and give your business partners and your customers what they want most: speed, convenience, and control over their transactions. Develop a robust strategy, one in which your company thrives whether blockchain is transformative or not.

The Roots of the Technology

Decentralized digital currency started in 2008 as a countercultural initiative. During its first few years, it was often described as a covert post–financial crisis protest against the global banking system, and bitcoins were used as an alternative currency by money launderers and illegal "dark Web" trading sites such as the "Silk Road" exchanges (which have been systematically shut down by legal authorities). The name of the bitcoin protocol's creator, Satoshi Nakamoto, is widely assumed to be a pseudonym, and a number of attempts to detect his or her real identity have proven inconclusive. Nakamoto published the specs for the bitcoin system in 2008, and opened the peer-to-peer software system in 2009. At the time, 1,000 bitcoins were worth less than US$3.

But digital currency was also recognized, from the start, as a potential wild card in legitimate finance — and as a possible investment vehicle. Its value began to rise rapidly after 2010. The currency reached its peak value on November 29, 2013, when a single bitcoin sold for $1,124.76. Since then, the price has stabilized considerably, hovering between $200 and $400 for most of 2015. The ultimate fate of the currency, including how broadly it will be accepted, is uncertain.

Anyone can try to create a bitcoin, but it's not easy. The technique for making bitcoins, known as "mining," was deliberately designed to protect the currency's value through scarcity. Bitcoins can be created only at a constrained rate — it takes about 10 minutes per coin,

on average — and each new bitcoin is slightly more difficult to create than the one that came before. The processing power required for each bitcoin is so large the currency has been criticized for contributing to climate change, because of the carbon burned in running bitcoin-mining computers. As a medium of exchange, the bitcoin, like the U.S. dollar or any other currency, has no intrinsic value. It can be bought or sold, but it is not automatically redeemable for another commodity, such as gold. However, whereas most currencies are backed by a government or central bank, bitcoin is authenticated by the peer network that produced it. Everyone who purchases a bitcoin knows that it is valid because the same distributed ledger has tracked it, and all other bitcoins, since each was created.

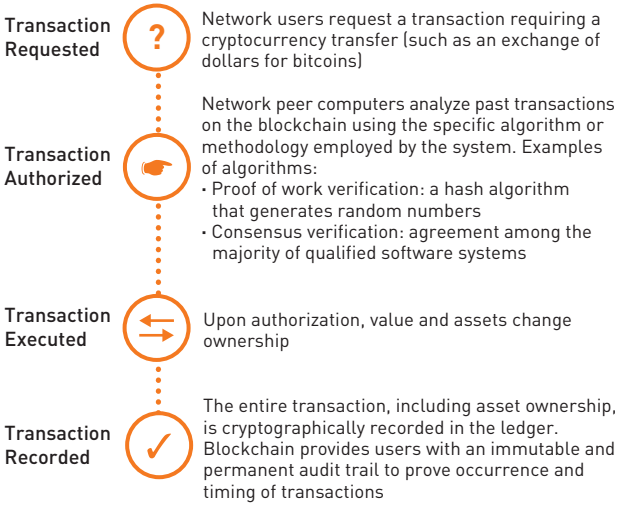
This distributed ledger — the first blockchain ledger ever created was for bitcoin, and it set the pattern for others — represents the most innovative and potentially influential aspect of the technology. Participants interact with one another using pseudonyms, and their real identities are encrypted. The ledger uses public-key encryption, which is virtually impossible to break, because a message can be unlocked only when a public and a private element (the latter held only by the recipient) are linked.

The term *blockchain* is derived from the way transactions are stored. For example, every time a bitcoin is created or changes hands, the ledger automatically creates a new transaction record composed of blocks of data, each encrypted by altering (or "hashing") part of the previous block. The cryptographic connection between each block and the next forms one link of the chain. This process compounds the mathematical difficulty of committing a successful fraud, because blocks of transactions, as well as individual transactions, are continuously validated. The algorithms also incorporate an ID for each buyer and seller in a transaction, adding those IDs to the block.

One of the most noteworthy features of the blockchain architecture is the decentralized technology, which helps ensure that a transaction is reliably reported. When a blockchain transaction (such as a bitcoin sale) takes place, a number of separate computers, connected across the network, process the algorithm and confirm one another's calculation. The record of transactions thus continually expands and is shared in real time by thousands of people (hence the name "distributed ledger"). The ledger stores basic information about each transaction — such as sender, receiver, time, asset type, and quantity. The blockchain process ensures validity, by mathematically linking each new transaction to those that came before it. This provides the evidence of the provenance of each transaction in a chain of records going back to the creation of the database, block of code after block after block (*see Exhibit 1*).

The combination of the ledger and the blockchain technology makes bitcoin — or any other system that uses that combination — a virtual, distributed, and decentralized entity. No one is needed to validate the transactions. This is why bitcoin is often referred to as a "trustless" system. You do not need to know anything about the other players, or trust them as individuals, to have faith in the system and invest your money there. Moreover, once committed to that distributed ledger,

Exhibit 1: **The Dynamics of a Blockchain (Distributed Ledger)**



Source: Strategy&

Whereas most currencies are backed by a government or central bank, bitcoin is authenticated by the peer network that produced it.

Exhibit 2: **The Blockchain Gang**

Here are some examples of the early efforts by banks and other financial-services companies to prototype activities involving blockchain and distributed ledger technology, or to explore how they might affect their operations and offerings.

BANKING SERVICES	
USAA	Reportedly exploring how blockchain technology can decentralize back-office operations; also participated in Coinbase's US$75 million Series C funding round
CBW Bank	Partnered with blockchain startup Ripple to use cryptocurrency for real-time cross-border payments
Barclays	Signed a deal with Safello, which operates an online exchange for bitcoin, to test combinations of traditional banking processes and blockchain technologies
Santander	Exploring use cases for blockchain technology; set up a $100 million financial technology (fintech) investment fund in 2014 and created a multimillion-dollar fund in 2015 to invest in and build fintech startups
Citi	Has built three separate internal blockchains within labs to test the technology, focusing primarily on international payments, followed by trading applications
INVESTMENT SERVICES AND CAPITAL MARKETS	
UBS	Opening a technology lab in London to explore using blockchain technology in financial services
Goldman Sachs	In April, led a $50 million funding round for Circle Internet Financial, a startup allowing customers to send and receive bitcoins, and to convert U.S. dollars into them
BNY Mellon	Created its own digital currency, BK coins, and built an employee recognition application that rewards IT staff with the tokens, which can be redeemed for gift cards and vouchers
Nasdaq	Implementing the bitcoin blockchain technology in its Nasdaq Private Market, a marketplace for pre-IPO trading, to expand and enhance the equity management capabilities it offers
TRANSACTION AND PAYMENT SERVICES	
American Express	CEO has acknowledged the disruptive potential of bitcoin and expressed interest in its underlying blockchain technology
First Data	Owner of Gyft, an online platform for buying, sending, and redeeming gift cards, which partnered with Chain, a blockchain startup, to run gift cards for thousands of small businesses on the peer network
PayPal	Partnered with BitPay, Coinbase, and GoCoin, three bitcoin startups, to allow its digital goods merchants to accept bitcoin payments
TECHNOLOGY COMPANIES	
IBM	Developing its own version of blockchain as an open-source software platform, for use as the backbone of a collaborative network sponsored by the Linux Foundation
Intel	Expressed an interest in conducting blockchain research and is reportedly developing related projects involving cryptographic researc; also a member of the Linux Foundation network

Source: Strategy&

If you're known for rapid fulfillment, the fast turnaround rates enabled by blockchain could allow you to stay ahead of competitors.

transactions are immutable. Records cannot be tampered with, because altering them would require coordinating many separate computers.

Impact and Innovation

If you are a senior executive in a financial-services firm, you may already be experimenting with distributed ledger technologies, if only to see how they fit with your strategy. You have lots of company. By 2014, more than a dozen major companies were actively exploring blockchain-related ventures and their potential effect on core practices (*see Exhibit 2, previous page*). For example, blockchain might streamline transaction processing by establishing a single source of truth, available to all, updated in near real time. This could increase the speed of exchange, reduce the number of intermediaries (and the costs associated with them), improve security, digitize assets, give wider access to people who don't have bank accounts, enable better bookkeeping, and improve regulatory compliance.

The technology could also be used to create and support "smart contracts": code-based, defined sets of rules that sit atop a blockchain database, and that execute only when specific actions occur. Eris Industries, a software firm that created one of the first blockchain-based platforms for this application, describes smart contracts as modular components, similar to apps on a financial network, that can be combined to provide verifiability to any type of transaction. According to the Eris website, the uses could be "as simple as upvoting a post on a forum, to the more complex such as loan collateralisation and futures contracts, to the highly complex such as repayment prioritisation on a structured note."

In fact, this technology could affect a wide range of offerings and practices in financial services:

- **Greater access to financial services in emerging economies.** Billions of people around the world lack access to banks and currency exchange. Blockchain-based distributed ledgers could change this. Just as the smartphone gave people without phone lines access to communication, information, and e-commerce, these technologies can provide a person the legitimacy needed to open a bank account or borrow money — without having to prove ownership of real estate or meeting other qualifications that are challenging in many countries.
- **Improved bookkeeping.** Companies can use the distributed, publicly verified, and nearly real-time ledger of transactions for bookkeeping, data mining, and records verification. This could reduce the effort spent on reconciling information among various computer systems. It could also link the systems to external information sources, such as pricing feeds (electronic vendors of trading data), in a more customizable and secure way.
- **More flexible reserves management.** Faster settlement and immediate notification would reduce the amount of cash and other collateral that a bank must hold to mitigate settlement risk. Blockchain's innately transparent tracking of capital flows could require banks to keep less money on reserve for working capital or foreign exchange capital needs.
- **More efficient regulatory compliance.** A central, immutable ledger of transactions would allow auditors and regulators to rapidly monitor the flow of financial data, avoiding after-the-fact verification.
- **Improvements in common business functions.** Management processes for accounts payable and re-

ceivables could be automated. New types of brokerage accounts, enabled by smart contracts, could allow buy-side institutions to trade directly with one another, or manage over-the-counter derivatives trading among a broad marketplace of players. Automated exchanges might take on some of the communications, settlement, and clearing functions that networks and central counterparties such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT), central banks, and payment networks perform now. There could also be blockchain-based vehicles for issuing new shares of stock, or overseeing retail transactions.

- **More startups in the distributed ledger domain.** A wide variety of ancillary businesses are rapidly emerging. Cryptocurrency exchanges, such as Armory and Coinbase, help their clients buy and sell cryptocurrency, store their holdings, manage the private encryption keys for those assets, and protect their currency holdings from online theft. (One favored approach is to keep the cryptocurrency stored on a dedicated computer that is not connected to the Internet.) Another company, Libra, helps corporations report, audit, and analyze digital asset transactions, regardless of the blockchain database used. Other startups, including Blockstream, Digital Asset Holdings, and itBit, facilitate digital asset transactions for banks and other financial institutions. And then there is Wallet Recovery Services, which helps the owner of a lost or forgotten password try to recover it through "brute force" decryption. This can be the only recourse for someone who kept their private encryption key in an electronic wallet on a smartphone, neglected to make a backup, and then lost the smartphone in a fire. (It's happened.) More startups are sure to appear offering other new blockchain-related services, including guidance to help people navigate all these unfamiliar systems.

Four Steps to a Blockchain-Enabled Strategy

Your blockchain and distributed ledger efforts will be most effective if you see them as ways to reinforce or strengthen your company's most distinctive capabilities — the ones that differentiate you in the market. For example, if you're known for rapid fulfillment and responsive customer service, the fast turnaround rates enabled by blockchain could allow you to stay ahead of competitors. At the same time, the technology is too new and unproven to base your company on. Therefore, your best investments are those that allow you to explore new approaches with strategic potential and understand the costs involved before committing to them.

We recommend creating a core technology working group to better understand the possibilities. But keep a close watch. Working groups like these can easily get caught up in the promise of new technologies, at the expense of your overarching strategy. To counter this tendency, they need to have a clear idea of your company's strategic goals, and how blockchain could enhance its value proposition — and then they need to constrain their efforts accordingly.

Step 1: Find specific opportunities. Charge the core technology working group with designing an effective path to the future. Start by compiling a list of potential pilot projects for which a distributed ledger could make a difference. One good place to start is with pain points: back-office workarounds, delays, and areas of client dissatisfaction. The working group should include (or consult with) a wide range of stakeholders and specialists from both inside and outside the organization, in order to compile a full list of strong prospects.

For example, a financial-services firm might try to use blockchain to improve risky or time-consuming business operations, such as reconciling cross-border payments to international subsidiaries. It might explore rethinking costly but necessary functions, such as compliance with anti–money laundering and know-your-customer regulations. There are many opportunities for streamlining operations, including transaction processing and the reconciliation of messages or data. The group could reduce the redundancy in data repositories, or look at identity issues, including the vulnerability of the company to cyber-attack. Or simply begin with consumer dissatisfaction, converting complaints to opportunities for improvement.

Your working group may be tempted to favor op-

tions that are most strongly linked to extreme disruption, or to the most talked-about technologies. But the press is often misleading, and technological change often takes place at a slower pace than people expect.

It's best to pick starting points that could most improve your own distinctive capabilities. For example, select pilot projects that show potential for helping you handle key business processes much faster than your competitors can.

Step 2: Explore feasibility and readiness. For each of the starting points you've chosen, develop explicit hypotheses describing how distributed ledger technologies can make a difference. For example, perhaps the finance function could engage with a distributed ledger provider such as Ripple or PeerNova to manage internal money movements among geographically dispersed legal entities. The hypothesis: It would decrease the time required for adjustments, reduce the need for adjustments, and increase transparency.

Or you might propose a smart contract test in your commercial banking function, using technology from startups such as Skuchain and Gazebo to simplify supply chain finance processes. If the test succeeds, you should see a certain level of cost reduction in a specified amount of time.

To solidify your hypotheses, once again consult with key business stakeholders. In addition to your internal business and functional teams, include customers in this group. Engage with people from risk management, regulatory compliance, operations, IT, finance, and tax, among others, so that your early proofs of concept don't require a restart after these stakeholders weigh in with their requirements.

Some of the factors to consider, as you solidify your hypotheses:

- **The degree to which the technology will remain hidden to end-users.** We recommend starting in the middle and back offices before moving to processes that are visible to customers.
- **The legislative and regulatory environment, and the way it affects bitcoin and distributed ledger technologies in those jurisdictions.** Some jurisdictions may have rules governing privacy and autonomy that could affect how you organize and disclose data.
- **Your competitive landscape.** Consider how other relevant market participants (such as suppliers, customers, and competitors) might adopt the technology, and over what time frame.
- **Your own capacity for change.** Some of these measures might require significant shifts in your operations, or a different cultural orientation within your company. Consider the ability of your institution to change business processes to take advantage of distributed ledger technologies.

At the end of this step, you should have narrowed your list down to a few possible starting points. They should be limited and tangible enough to provide a good test of the technology — while also being relevant to your core business. And you should have a clear idea of how to develop prototype experiments for each of them.

Step 3: Put your prototypes to work. As you move into implementation, you will adjust your parameters to make the prototypes work. Inevitably, people will improve your practices during the testing and evaluation process. You'll also discover new ways to apply the prototype's blockchain innovations, putting you in a better position to make strategic decisions.

But stay true to your original hypotheses. Make sure that no matter how the prototype is altered, it remains relevant to your firm's strategy and the distinctive capabilities that propel you forward. Monitor results frequently enough to get a clear sense of your momentum. If you don't reach the milestones you expect, ask why, and keep refining and testing.

Also, make it a fair test. Don't put laggards, who are predisposed to the status quo, in charge of implementation. Pick leaders who are reasonably skeptical, but who have a clear understanding of the new technologies, and who are open to their promise. When hiring external consultants and technology providers, choose those who demonstrably understand your company's strategic direction — not just their own technological

When faced with disruptive technologies, the most effective companies thrive by incorporating them into the way they do business.

agenda — and who are ready to help you move there. Settle on a development time frame that is long enough to help you reasonably assess the outcomes.

Step 4: Scale your efforts appropriately. With any luck, your prototype experiments will result in some immediate, tangible improvements that justify your interest in blockchain. They may also expand your awareness of its potential and what it will cost to implement real change.

Now focus on its impact on your core business. Will this change the way you do business with the parties you work with most consistently? For example, if you're a custody bank, set up to manage financial holdings such as securities and commodities, would blockchain technologies help you manage the most important asset classes more effectively?

Develop a long-term plan based on the results of the first prototypes. Select a few long-range goals — increased revenue, better compliance, cost reductions, quality improvements — and agree upon them. Create a road map for scaling up in a measurable, achievable, and worthwhile way.

It should be clearer at this point how much this technology will affect your core business practices. If it stays on the periphery, affecting relatively few customers, you will be glad you limited your investment to a few prototypes. However, if it moves into the mainstream of your business, then it could change everything. If that happens, by having invested in these prototypes, you'll be prepared. You can scale up your prototypes to take advantage of everything blockchain offers.

When faced with disruptive technologies, the most effective companies thrive by incorporating them into the way they do business. Distributed ledger technologies could offer financial-services institutions a once-in-a-generation opportunity to transform themselves. This technology could also create powerful opportunities in other industries. Connected-car and auto-sharing innovations emerged more than a decade after GPS became popular; years from now, there may be similar innovations that take advantage of blockchain. Companies that adjust their business models accordingly may well enjoy enormous rewards, including increased transparency, lower costs, and greater time efficiencies. Your challenge is to understand the technology well enough, and rapidly enough, to bet a bit of your future on it — without putting your entire enterprise at risk. +

Reprint No. 16111

Resources

Betsy Burton and David A. Willis, *Gartner's Hype Cycles for 2015: Five Megatrends Shift the Computing Landscape,* Aug. 12, 2015: Gartner Group predicts that cryptocurrencies will reach a "plateau of productivity" in two to five years.

Charity Delich, "Best of Multimedia: Bitcoin's Turbulent History," *s+b,* Mar. 14, 2014: Links to a comprehensive timeline of this technology.

Andrew Haldane, "How Low Can You Go?" Sept. 18, 2015: Speech given by the Bank of England's chief economist, on the future of central banks, discussing blockchain as a disruptive force.

PwC Financial Services Institute, "Money Is No Object: Understanding the Evolving Cryptocurrency Market," PwC, Aug. 2015: Definitive report on cryptocurrency, who is using it, and how it could evolve.

Michael Santoli, "Currency Events," *s+b,* June 30, 2015: Review of *Digital Gold,* Nathaniel Popper's engaging history of bitcoin and related technologies.

More thought leadership on this topic:
strategy-business.com/technology

strategy+business magazine
is published by certain member firms
of the PwC network.
To subscribe, visit strategy-business.com
or call 1-855-869-4862.

- strategy-business.com
- facebook.com/strategybusiness
- linkedin.com/company/strategy-business
- twitter.com/stratandbiz

pwc | strategy&