**R3 CEV**<http://r3cev.com/>

Understanding Blockchain

<http://www.iftf.org/future-now/article-detail/understand-the-blockchain-in-two-minutes/>

The Economist

<http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>

**The promise of the blockchain**

**The trust machine**

**The technology behind bitcoin could transform how the economy works**

Oct 31st 2015 | [From the print edition](http://www.economist.com/printedition/2015-10-31)

* [imekeeper](http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine)



BITCOIN has a bad reputation. The decentralised digital cryptocurrency, powered by a vast computer network, is notorious for the wild fluctuations in its value, the zeal of its supporters and its degenerate uses, such as extortion, buying drugs and hiring hitmen in the online bazaars of the “dark net”.

This is unfair. The value of a bitcoin has been pretty stable, at around $250, for most of this year. Among regulators and financial institutions, scepticism has given way to enthusiasm (the European Union recently recognised it as a currency). But most unfair of all is that bitcoin’s shady image causes people to overlook the extraordinary potential of the “blockchain”, the technology that underpins it. This innovation carries a significance stretching far beyond cryptocurrency. The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust.

The blockchain food chain

|  |
| --- |
|  |

To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the bitcoin currency, the specific blockchain that underpins it and the idea of blockchains in general. A helpful analogy is with Napster, the pioneering but illegal “peer-to-peer” file-sharing service that went on line in 1999, providing free access to millions of music tracks. Napster itself was swiftly shut down, but it inspired a host of other peer-to-peer services. Many of these were also used for pirating music and films. Yet despite its dubious origins, peer-to-peer technology found legitimate uses, powering internet startups such as Skype (for telephony) and Spotify (for music streaming)—and also, as it happens, bitcoin.

The blockchain is an even more potent technology. In essence it is a shared, trusted, public ledger that everyone can inspect, but which no single user controls. The participants in a blockchain system collectively keep the ledger up to date: it can be amended only according to strict rules and by general agreement. Bitcoin’s blockchain ledger prevents double-spending and keeps track of transactions continuously. It is what makes possible a currency without a central bank.

Blockchains are also the latest example of the unexpected fruits of cryptography. Mathematical scrambling is used to boil down an original piece of information into a code, known as a hash. Any attempt to tamper with any part of the blockchain is apparent immediately—because the new hash will not match the old ones. In this way a science that keeps information secret (vital for encrypting messages and online shopping and banking) is, paradoxically, also a tool for open dealing.

Bitcoin itself may never be more than a curiosity. However blockchains have a host of other uses because they meet the need for a trustworthy record, something vital for transactions of every sort. Dozens of startups now hope to capitalise on the blockchain technology, either by doing clever things with the bitcoin blockchain or by creating new blockchains of their own (see [article](http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable" \t "_blank)).

One idea, for example, is to make cheap, tamper-proof public databases—land registries, say, (Honduras and Greece are interested); or registers of the ownership of luxury goods or works of art. Documents can be notarised by embedding information about them into a public blockchain—and you will no longer need a notary to vouch for them. Financial-services firms are contemplating using blockchains as a record of who owns what instead of having a series of internal ledgers. A trusted private ledger removes the need for reconciling each transaction with a counterparty, it is fast and it minimises errors. Santander reckons that it could save banks up to $20 billion a year by 2022. Twenty-five banks have just joined a blockchain startup, called R3 CEV, to develop common standards, and NASDAQ is about to start using the technology to record trading in securities of private companies.

These new blockchains need not work in exactly the way that bitcoin’s does. Many of them could tweak its model by, for example, finding alternatives to its energy-intensive “mining” process, which pays participants newly minted bitcoins in return for providing the computing power needed to maintain the ledger. A group of vetted participants within an industry might instead agree to join a private blockchain, say, that needs less security. Blockchains can also implement business rules, such as transactions that take place only if two or more parties endorse them, or if another transaction has been completed first. As with Napster and peer-to-peer technology, a clever idea is being modified and improved. In the process, it is fast throwing off its reputation for shadiness.

New chains on the block

The spread of blockchains is bad for anyone in the “trust business”—the centralised institutions and bureaucracies, such as banks, clearing houses and government authorities that are deemed sufficiently trustworthy to handle transactions. Even as some banks and governments explore the use of this new technology, others will surely fight it. But given the decline in trust in governments and banks in recent years, a way to create more scrutiny and transparency could be no bad thing.

Drawing up regulations for blockchains at this early stage would be a mistake: the history of peer-to-peer technology suggests that it is likely to be several years before the technology’s full potential becomes clear. In the meantime regulators should stay their hands, or find ways to accommodate new approaches within existing frameworks, rather than risk stifling a fast-evolving idea with overly prescriptive rules.

The notion of shared public ledgers may not sound revolutionary or sexy. Neither did double-entry book-keeping or joint-stock companies. Yet, like them, the blockchain is an apparently mundane process that has the potential to transform how people and businesses co-operate. Bitcoin fanatics are enthralled by the libertarian ideal of a pure, digital currency beyond the reach of any central bank. The real innovation is not the digital coins themselves, but the trust machine that mints them—and which promises much more besides.

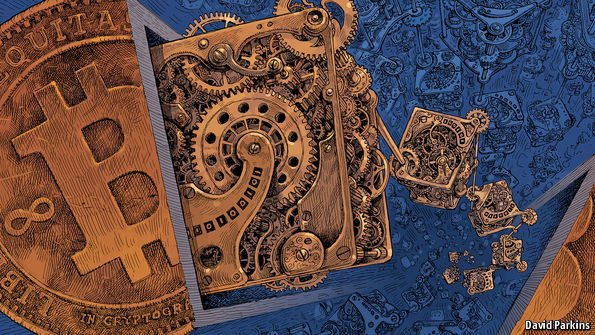
**Blockchains**

**The great chain of being sure about things**

**The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the cryptocurrency**

Oct 31st 2015 | [From the print edition](http://www.economist.com/printedition/2015-10-31)

* [imekeeper](http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable)



WHEN the Honduran police came to evict her in 2009 Mariana Catalina Izaguirre had lived in her lowly house for three decades. Unlike many of her neighbours in Tegucigalpa, the country’s capital, she even had an official title to the land on which it stood. But the records at the country’s Property Institute showed another person registered as its owner, too—and that person convinced a judge to sign an eviction order. By the time the legal confusion was finally sorted out, Ms Izaguirre’s house had been demolished.

It is the sort of thing that happens every day in places where land registries are badly kept, mismanaged and/or corrupt—which is to say across much of the world. This lack of secure property rights is an endemic source of insecurity and injustice. It also makes it harder to use a house or a piece of land as collateral, stymying investment and job creation.

Related topics

* [Bitcoins](http://www.economist.com/topics/bitcoins)

Such problems seem worlds away from bitcoin, a currency based on clever cryptography which has a devoted following among mostly well-off, often anti-government and sometimes criminal geeks. But the cryptographic technology that underlies bitcoin, called the “blockchain”, has applications well beyond cash and currency. It offers a way for people who do not know or trust each other to create a record of who owns what that will compel the assent of everyone concerned. It is a way of making and preserving truths.

That is why politicians seeking to clean up the Property Institute in Honduras have asked Factom, an American startup, to provide a prototype of a blockchain-based land registry. Interest in the idea has also been expressed in Greece, which has no proper land registry and where only 7% of the territory is adequately mapped.

A place in the past

Other applications for blockchain and similar “distributed ledgers” range from thwarting diamond thieves to streamlining stockmarkets: the NASDAQ exchange will soon start using a blockchain-based system to record trades in privately held companies. The Bank of England, not known for technological flights of fancy, seems electrified: distributed ledgers, it concluded in a research note late last year, are a “significant innovation” that could have “far-reaching implications” in the financial industry.

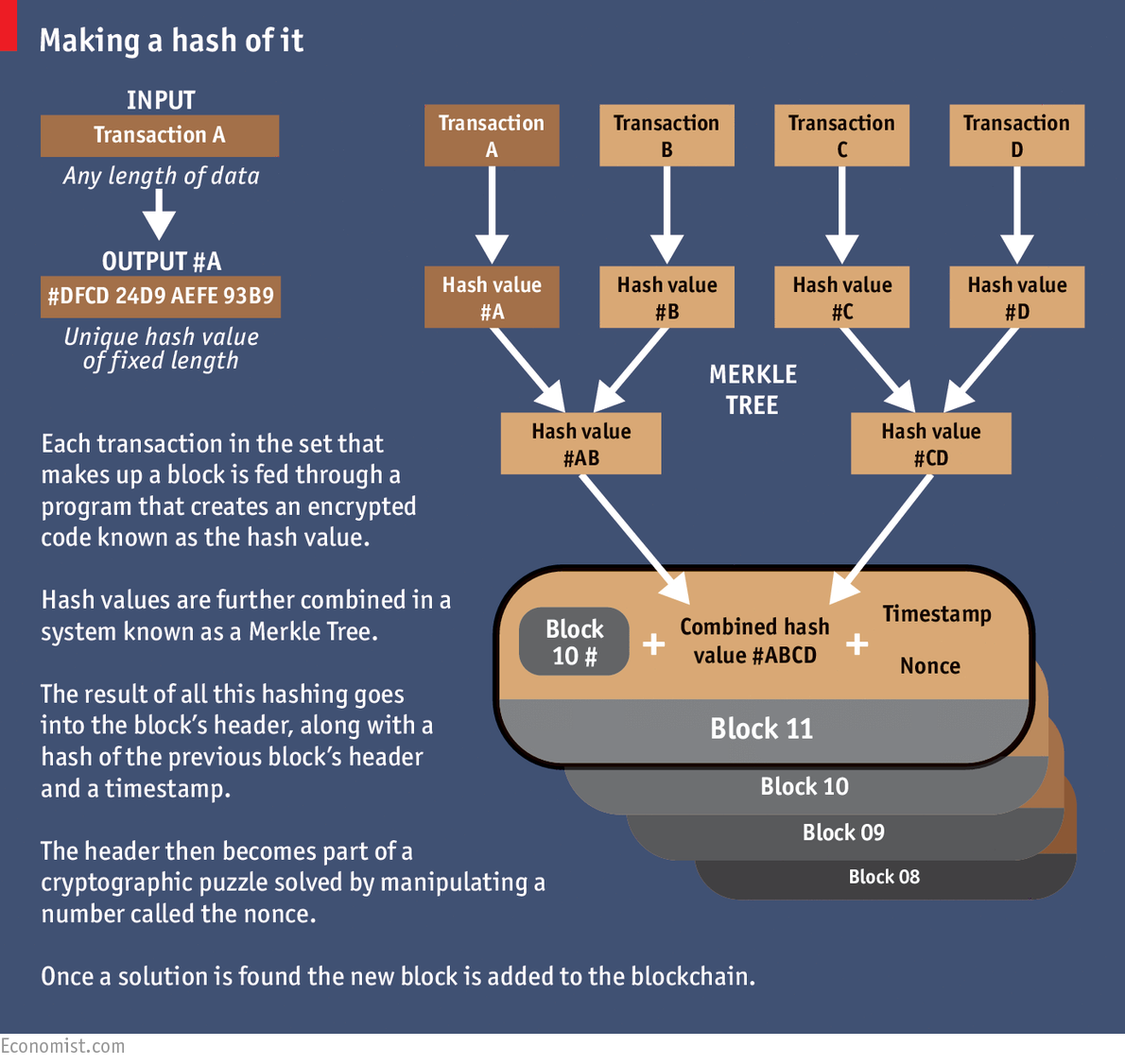
The politically minded see the blockchain reaching further than that. When co-operatives and left-wingers gathered for this year’s OuiShare Fest in Paris to discuss ways that grass-roots organisations could undermine giant repositories of data like Facebook, the blockchain made it into almost every speech. Libertarians dream of a world where more and more state regulations are replaced with private contracts between individuals—contracts which blockchain-based programming would make self-enforcing.

The blockchain began life in the mind of Satoshi Nakamoto, the brilliant, pseudonymous and so far unidentified creator of bitcoin—a “purely peer-to-peer version of electronic cash”, as he put it in a paper published in 2008. To work as cash, bitcoin had to be able to change hands without being diverted into the wrong account and to be incapable of being spent twice by the same person. To fulfil Mr Nakamoto’s dream of a decentralised system the avoidance of such abuses had to be achieved without recourse to any trusted third party, such as the banks which stand behind conventional payment systems.

It is the blockchain that replaces this trusted third party. A database that contains the payment history of every bitcoin in circulation, the blockchain provides proof of who owns what at any given juncture. This distributed ledger is replicated on thousands of computers—bitcoin’s “nodes”—around the world and is publicly available. But for all its openness it is also trustworthy and secure. This is guaranteed by the mixture of mathematical subtlety and computational brute force built into its “consensus mechanism”—the process by which the nodes agree on how to update the blockchain in the light of bitcoin transfers from one person to another.

Let us say that Alice wants to pay Bob for services rendered. Both have bitcoin “wallets”—software which accesses the blockchain rather as a browser accesses the web, but does not identify the user to the system. The transaction starts with Alice’s wallet proposing that the blockchain be changed so as to show Alice’s wallet a little emptier and Bob’s a little fuller.

The network goes through a number of steps to confirm this change. As the proposal propagates over the network the various nodes check, by inspecting the ledger, whether Alice actually has the bitcoin she now wants to spend. If everything looks kosher, specialised nodes called miners will bundle Alice’s proposal with other similarly reputable transactions to create a new block for the blockchain.



This entails repeatedly feeding the data through a cryptographic “hash” function which boils the block down into a string of digits of a given length (see diagram). Like a lot of cryptography, this hashing is a one-way street. It is easy to go from the data to their hash; impossible to go from the hash back to the data. But though the hash does not contain the data, it is still unique to them. Change what goes into the block in any way—alter a transaction by a single digit—and the hash would be different.

Running in the shadows

That hash is put, along with some other data, into the header of the proposed block. This header then becomes the basis for an exacting mathematical puzzle which involves using the hash function yet again. This puzzle can only be solved by trial and error. Across the network, miners grind through trillions and trillions of possibilities looking for the answer. When a miner finally comes up with a solution other nodes quickly check it (that’s the one-way street again: solving is hard but checking is easy), and each node that confirms the solution updates the blockchain accordingly. The hash of the header becomes the new block’s identifying string, and that block is now part of the ledger. Alice’s payment to Bob, and all the other transactions the block contains, are confirmed.

This puzzle stage introduces three things that add hugely to bitcoin’s security. One is chance. You cannot predict which miner will solve a puzzle, and so you cannot predict who will get to update the blockchain at any given time, except in so far as it has to be one of the hard working miners, not some random interloper. This makes cheating hard.

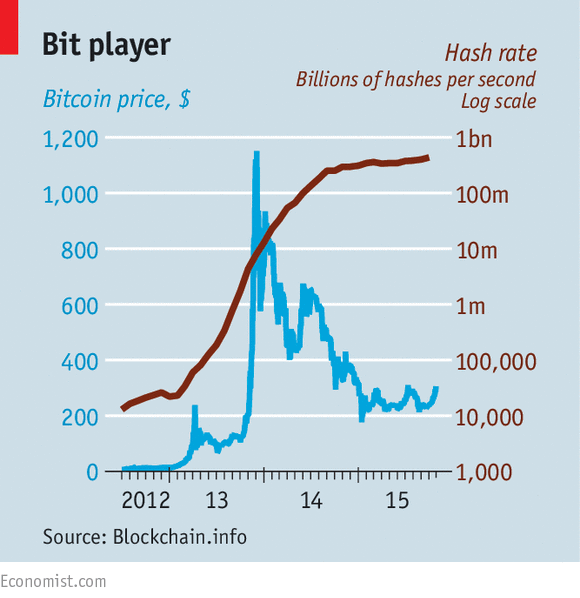
The second addition is history. Each new header contains a hash of the previous block’s header, which in turn contains a hash of the header before that, and so on and so on all the way back to the beginning. It is this concatenation that makes the blocks into a chain. Starting from all the data in the ledger it is trivial to reproduce the header for the latest block. Make a change anywhere, though—even back in one of the earliest blocks—and that changed block’s header will come out different. This means that so will the next block’s, and all the subsequent ones. The ledger will no longer match the latest block’s identifier, and will be rejected.

Is there a way round this? Imagine that Alice changes her mind about paying Bob and tries to rewrite history so that her bitcoin stays in her wallet. If she were a competent miner she could solve the requisite puzzle and produce a new version of the blockchain. But in the time it took her to do so, the rest of the network would have lengthened the original blockchain. And nodes always work on the longest version of the blockchain there is. This rule stops the occasions when two miners find the solution almost simultaneously from causing anything more than a temporary fork in the chain. It also stops cheating. To force the system to accept her new version Alice would need to lengthen it faster than the rest of the system was lengthening the original. Short of controlling more than half the computers—known in the jargon as a “51% attack”—that should not be possible.

Dreams are sometimes catching

Leaving aside the difficulties of trying to subvert the network, there is a deeper question: why bother to be part of it at all? Because the third thing the puzzle-solving step adds is an incentive. Forging a new block creates new bitcoin. The winning miner earns 25 bitcoin, worth about $7,500 at current prices.

All this cleverness does not, in itself, make bitcoin a particularly attractive currency. Its value is unstable and unpredictable (see chart), and the total amount in circulation is deliberately limited. But the blockchain mechanism works very well. According to blockchain.info, a website that tracks such things, on an average day more than 120,000 transactions are added to the blockchain, representing about $75m exchanged. There are now 380,000 blocks; the ledger weighs in at nearly 45 gigabytes.



Most of the data in the blockchain are about bitcoin. But they do not have to be. Mr Nakamoto has built what geeks call an “open platform”—a distributed system the workings of which are open to examination and elaboration. The paragon of such platforms is the internet itself; other examples include operating systems like Android or Windows. Applications that depend on basic features of the blockchain can thus be developed without asking anybody for permission or paying anyone for the privilege. “The internet finally has a public data base,” says Chris Dixon of Andreessen Horowitz, a venture-capital firm which has financed several bitcoin start-ups, including Coinbase, which provides wallets, and 21, which makes bitcoin-mining hardware for the masses.

For now blockchain-based offerings fall in three buckets. The first takes advantage of the fact that any type of asset can be transferred using the blockchain. One of the startups betting on this idea is Colu. It has developed a mechanism to “dye” very small bitcoin transactions (called “bitcoin dust”) by adding extra data to them so that they can represent bonds, shares or units of precious metals.

Protecting land titles is an example of the second bucket: applications that use the blockchain as a truth machine. Bitcoin transactions can be combined with snippets of additional information which then also become embedded in the ledger. It can thus be a registry of anything worth tracking closely. Everledger uses the blockchain to protect luxury goods; for example it will stick on to the blockchain data about a stone’s distinguishing attributes, providing unchallengeable proof of its identity should it be stolen. Onename stores personal information in a way that is meant to do away with the need for passwords; CoinSpark acts as a notary. Note, though, that for these applications, unlike for pure bitcoin transactions, a certain amount of trust is required; you have to believe the intermediary will store the data accurately.

It is the third bucket that contains the most ambitious applications: “smart contracts” that execute themselves automatically under the right circumstances. Bitcoin can be “programmed” so that it only becomes available under certain conditions. One use of this ability is to defer the payment miners get for solving a puzzle until 99 more blocks have been added—which provides another incentive to keep the blockchain in good shape.

Lighthouse, a project started by Mike Hearn, one of bitcoin’s leading programmers, is a decentralised crowdfunding service that uses these principles. If enough money is pledged to a project it all goes through; if the target is never reached, none does. Mr Hearn says his scheme will both be cheaper than non-bitcoin competitors and also more independent, as governments will be unable to pull the plug on a project they don’t like.

Energy is contagious

The advent of distributed ledgers opens up an “entirely new quadrant of possibilities”, in the words of Albert Wenger of USV, a New York venture firm that has invested in startups such as OpenBazaar, a middleman-free peer-to-peer marketplace. But for all that the blockchain is open and exciting, sceptics argue that its security may yet be fallible and its procedures may not scale. What works for bitcoin and a few niche applications may be unable to support thousands of different services with millions of users.

Though Mr Nakamoto’s subtle design has so far proved impregnable, academic researchers have identified tactics that might allow a sneaky and well financed miner to compromise the block chain without direct control of 51% of it. And getting control of an appreciable fraction of the network’s resources looks less unlikely than it used to. Once the purview of hobbyists, bitcoin mining is now dominated by large “pools”, in which small miners share their efforts and rewards, and the operators of big data centres, many based in areas of China, such as Inner Mongolia, where electricity is cheap.

Another worry is the impact on the environment. With no other way to establish the bona fides of miners, the bitcoin architecture forces them to do a lot of hard computing; this “proof of work”, without which there can be no reward, insures that all concerned have skin in the game. But it adds up to a lot of otherwise pointless computing. According to blockchain.info the network’s miners are now trying 450 thousand trillion solutions per second. And every calculation takes energy.

Because miners keep details of their hardware secret, nobody really knows how much power the network consumes. If everyone were using the most efficient hardware, its annual electricity usage might be about two terawatt-hours—a bit more than the amount used by the 150,000 inhabitants of King’s County in California’s Central Valley. Make really pessimistic assumptions about the miners’ efficiency, though, and you can get the figure up to 40 terawatt-hours, almost two-thirds of what the 10m people in Los Angeles County get through. That surely overstates the problem; still, the more widely people use bitcoin, the worse the waste could get.

Yet for all this profligacy bitcoin remains limited. Because Mr Nakamoto decided to cap the size of a block at one megabyte, or about 1,400 transactions, it can handle only around seven transactions per second, compared to the 1,736 a second Visa handles in America. Blocks could be made bigger; but bigger blocks would take longer to propagate through the network, worsening the risks of forking.

Earlier platforms have surmounted similar problems. When millions went online after the invention of the web browser in the 1990s pundits predicted the internet would grind to a standstill: *eppur si muove*. Similarly, the bitcoin system is not standing still. Specialised mining computers can be very energy efficient, and less energy-hungry alternatives to the proof-of-work mechanism have been proposed. Developers are also working on an add-on called “Lightning” which would handle large numbers of smaller transactions outside the blockchain. Faster connections will let bigger blocks propagate as quickly as small ones used to.

The problem is not so much a lack of fixes. It is that the network’s “bitcoin improvement process” makes it hard to choose one. Change requires community-wide agreement, and these are not people to whom consensus comes easily. Consider the civil war being waged over the size of blocks. One camp frets that quickly increasing the block size will lead to further concentration in the mining industry and turn bitcoin into more of a conventional payment processor. The other side argues that the system could crash as early as next year if nothing is done, with transactions taking hours.

A break in the battle

Mr Hearn and Gavin Andresen, another bitcoin grandee, are leaders of the big-block camp. They have called on mining firms to install a new version of bitcoin which supports a much bigger block size. Some miners who do, though, appear to be suffering cyber-attacks. And in what seems a concerted effort to show the need for, or the dangers of, such an upgrade, the system is being driven to its limits by vast numbers of tiny transactions.

This has all given new momentum to efforts to build an alternative to the bitcoin blockchain, one that might be optimised for the storing of distributed ledgers rather than for the running of a cryptocurrency. MultiChain, a build-your-own-blockchain platform offered by Coin Sciences, another startup, demonstrates what is possible. As well as offering the wherewithal to build a public blockchain like bitcoin’s, it can also be used to build private chains open only to vetted users. If all the users start off trusted the need for mining and proof-of-work is reduced or eliminated, and a currency attached to the ledger becomes an optional extra.

The first industry to adopt such sons of blockchain may well be the one whose failings originally inspired Mr Nakamoto: finance. In recent months there has been a rush of bankerly enthusiasm for private blockchains as a way of keeping tamper-proof ledgers. One of the reasons, irony of ironies, is that this technology born of anti-government libertarianism could make it easier for the banks to comply with regulatory requirements on knowing their customers and anti-money-laundering rules. But there is a deeper appeal.

Industrial historians point out that new powers often become available long before the processes that best use them are developed. When electric motors were first developed they were deployed like the big hulking steam engines that came before them. It took decades for manufacturers to see that lots of decentralised electric motors could reorganise every aspect of the way they made things. In its report on digital currencies, the Bank of England sees something similar afoot in the financial sector. Thanks to cheap computing financial firms have digitised their inner workings; but they have not yet changed their organisations to match. Payment systems are mostly still centralised: transfers are cleared through the central bank. When financial firms do business with each other, the hard work of synchronising their internal ledgers can take several days, which ties up capital and increases risk.

Distributed ledgers that settle transactions in minutes or seconds could go a long way to solving such problems and fulfilling the greater promise of digitised banking. They could also save banks a lot of money: according to Santander, a bank, by 2022 such ledgers could cut the industry’s bills by up to $20 billion a year. Vendors still need to prove that they could deal with the far-higher-than-bitcoin transaction rates that would be involved; but big banks are already pushing for standards to shape the emerging technology. One of them, UBS, has proposed the creation of a standard “settlement coin”. The first order of business for R3 CEV, a blockchain startup in which UBS has invested alongside Goldman Sachs, JPMorgan and 22 other banks, is to develop a standardised architecture for private ledgers.

The banks’ problems are not unique. All sorts of companies and public bodies suffer from hard-to-maintain and often incompatible databases and the high transaction costs of getting them to talk to each other. This is the problem Ethereum, arguably the most ambitious distributed-ledger project, wants to solve. The brainchild of Vitalik Buterin, a 21-year-old Canadian programming prodigy, Ethereum’s distributed ledger can deal with more data than bitcoin’s can. And it comes with a programming language that allows users to write more sophisticated smart contracts, thus creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level. Such cleverness, Mr Buterin hopes, will allow the formation of “decentralised autonomous organisations”—virtual companies that are basically just sets of rules running on Ethereum’s blockchain.



One of the areas where such ideas could have radical effects is in the “internet of things”—a network of billions of previously mute everyday objects such as fridges, doorstops and lawn sprinklers. A recent report from IBM entitled “Device Democracy” argues that it would be impossible to keep track of and manage these billions of devices centrally, and unwise to to try; such attempts would make them vulnerable to hacking attacks and government surveillance. Distributed registers seem a good alternative.

The sort of programmability Ethereum offers does not just allow people’s property to be tracked and registered. It allows it to be used in new sorts of ways. Thus a car-key embedded in the Ethereum blockchain could be sold or rented out in all manner of rule-based ways, enabling new peer-to-peer schemes for renting or sharing cars. Further out, some talk of using the technology to make by-then-self-driving cars self-owning, to boot. Such vehicles could stash away some of the digital money they make from renting out their keys to pay for fuel, repairs and parking spaces, all according to preprogrammed rules.

What would Rousseau have said?

Unsurprisingly, some think such schemes overly ambitious. Ethereum’s first (“genesis”) block was only mined in August and, though there is a little ecosystem of start-ups clustered around it, Mr Buterin admitted in a recent blog post that it is somewhat short of cash. But the details of which particular blockchains end up flourishing matter much less than the broad enthusiasm for distributed ledgers that is leading both start-ups and giant incumbents to examine their potential. Despite society’s inexhaustible ability to laugh at accountants, the workings of ledgers really do matter.

Today’s world is deeply dependent on double-entry book-keeping. Its standardised system of recording debits and credits is central to any attempt to understand a company’s financial position. Whether modern capitalism absolutely required such book-keeping in order to develop, as Werner Sombart, a German sociologist, claimed in the early 20th century, is open to question. Though the system began among the merchants of renaissance Italy, which offers an interesting coincidence of timing, it spread round the world much more slowly than capitalism did, becoming widely used only in the late 19th century. But there is no question that the technique is of fundamental importance not just as a record of what a company does, but as a way of defining what one can be.

Ledgers that no longer need to be maintained by a company—or a government—may in time spur new changes in how companies and governments work, in what is expected of them and in what can be done without them. A realisation that systems without centralised record-keeping can be just as trustworthy as those that have them may bring radical change.

Such ideas can expect some eye-rolling—blockchains are still a novelty applicable only in a few niches, and the doubts as to how far they can spread and scale up may prove well founded. They can also expect resistance. Some of bitcoin’s critics have always seen it as the latest techy attempt to spread a “Californian ideology” which promises salvation through technology-induced decentralisation while ignoring and obfuscating the realities of power—and happily concentrating vast wealth in the hands of an elite. The idea of making trust a matter of coding, rather than of democratic politics, legitimacy and accountability, is not necessarily an appealing or empowering one.

At the same time, a world with record-keeping mathematically immune to manipulation would have many benefits. Evicted Ms Izaguirre would be better off; so would many others in many other settings. If blockchains have a fundamental paradox, it is this: by offering a way of setting the past and present in cryptographic stone, they could make the future a very different place.

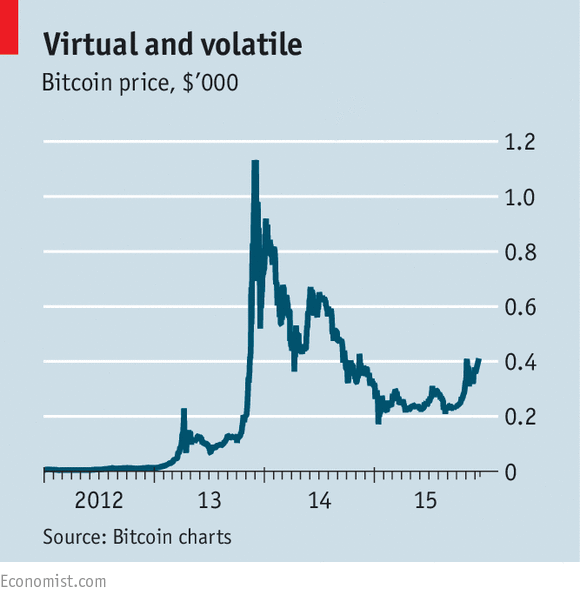
The Economist

## Bitcoin’s schism

### Stumbling blocks

# A split of the digital currency now seems unlikely, but problems remain

Dec 12th 2015 | HONG KONG | [From the print edition](http://www.economist.com/printedition/2015-12-12)



“IT’S time for a group hug,” one of the participants joked at the end. After a long and lively exchange, programmers, who write the software behind bitcoin, and “miners”, whose computers mint the digital currency, had indeed found some common ground. But the rapport between the two camps still seemed tentative. At one point a developer asked whether miners, who now mostly hail from China, would ever collude to steal bitcoin.

Suspicions between developers and miners were not the only ones on display at “Scaling Bitcoin”, a conference in Hong Kong this week. Developers themselves have been feuding, too. The event was intended to end a dispute about how to expand the capacity of the bitcoin system. Currently, it can only handle seven transactions per second—a fraction of what conventional payment systems can manage. The number could be increased by allowing bigger “blocks”—the name given to the batches into which bitcoin transactions are assembled before they are processed.

For years developers have disagreed about how much, if at all, blocks should grow. Fearing that the system would soon hit its limits, two of them, Gavin Andresen and Mike Hearn, lost patience this summer: they called on miners to install a new version of bitcoin’s software which works with much bigger blocks. The result was a rift between developers and a spasm in bitcoin’s yo-yoing value (see chart).

Highly technical talks, lengthy debates and much socialising allowed the more than 200 participants at the conference to air their grievances and discuss all sorts of ways to allow bitcoin to grow. It helped that the two renegades did not attend (Mr Andresen is now a researcher at MIT’s Media Lab and Mr Hearn has joined R3 CEV, a coalition of banks developing bitcoin-like technology). Bitcoin XT, as the controversial new software is called, has not been widely adopted.

Although details still need to be worked out, it now looks likely that developers will first—perhaps within a few months—implement technical fixes to boost bitcoin’s capacity without increasing the maximum block size. A small increase in the block size—probably from one to as many as four megabytes—is expected to come only later; it is considered a risky move that requires all computers on the bitcoin network to install new software at the same time.

That still leaves open the question of how such decisions should be made in future. Civil wars and subsequent peace conferences are an inefficient way to create consensus. As befits advocates of a currency without a central bank, neither developers nor miners want to be at the helm (in practice they share authority, since the system could not work without both groups). Some at the conference argued that, like the internet, bitcoin needs a formal governance structure. Others presented complex technical solutions that would allow market forces to decide how big blocks should be.

Behind such debates lurks a bigger question: what does bitcoin want to be when it grows up? Should it be immutable, like gold, or should it adapt to the demands of its users, even if that means becoming more like a conventional payment system? Perhaps Satoshi Nakamoto, the mysterious creator of bitcoin, could provide guidance. Reports this week suggested he may be an Australian academic under investigation by the taxman.

Welcome to strategy+business. [Here’s what’s new.](http://www.strategy-business.com/whats-new)

[](http://www.strategy-business.com)

Published: January 11, 2016

[Technology](http://www.strategy-business.com/technology)

# A Strategist’s Guide to Blockchain

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

by [John Plansky](http://www.strategy-business.com/author?author=John+Plansky), [Tim O’Donnell](http://www.strategy-business.com/author?author=Tim+O%E2%80%99Donnell), and [Kimberly Richards](http://www.strategy-business.com/author?author=Kimberly+Richards)



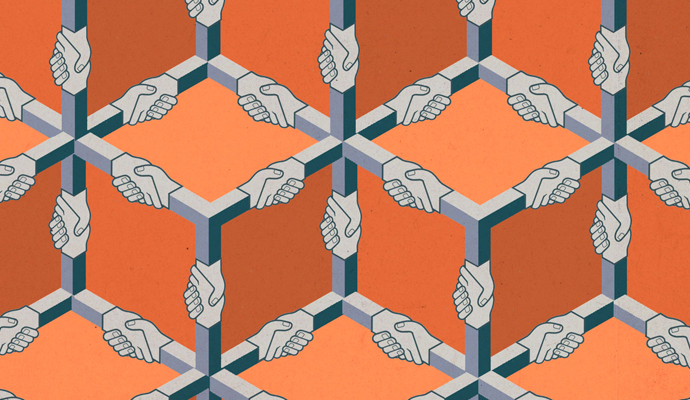


Illustration by Dan Page

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.

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

Blockchain could become a force anywhere trading occurs, trust is at a premium, and people need protection from identity theft.

But although the potential is immense, so is the uncertainty. Distributed ledger technologies are so new, so complex, and so prone to rapid change 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 crypto-currency 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.

## Related Stories

* [](https://www.pwc.com/us/en/financial-services/publications/assets/pwc-cryptocurrency-evolution.pdf)

### [Money is no object: Understanding the evolving cryptocurrency market](https://www.pwc.com/us/en/financial-services/publications/assets/pwc-cryptocurrency-evolution.pdf" \t "_blank)

* [](http://www.strategy-business.com/blog/Best-of-Multimedia-Bitcoins-Turbulent-History)

### [Best of Multimedia: Bitcoin’s Turbulent History](http://www.strategy-business.com/blog/Best-of-Multimedia-Bitcoins-Turbulent-History)

by Charity Delich

* [](http://www.strategy-business.com/blog/Driving-Digitization-in-Retail-Banking)

### [Driving Digitization in Retail Banking](http://www.strategy-business.com/blog/Driving-Digitization-in-Retail-Banking)

by Martin Roets

* [](http://www.strategy-business.com/article/00206)

### [To an Analog Banker in a Digital World](http://www.strategy-business.com/article/00206)

by Catherine Palmieri

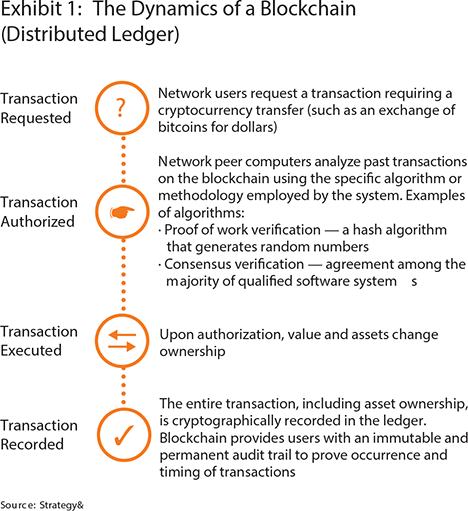
But digital currency was also recognized, from the start, as a potential wild card in legitimate finance — and as a possible investment vehicle. Its value began to rise rapidly after 2010. The currency reached its peak value on November 29, 2013, when a single bitcoin sold for $1,124.76. Since then, 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 the 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).

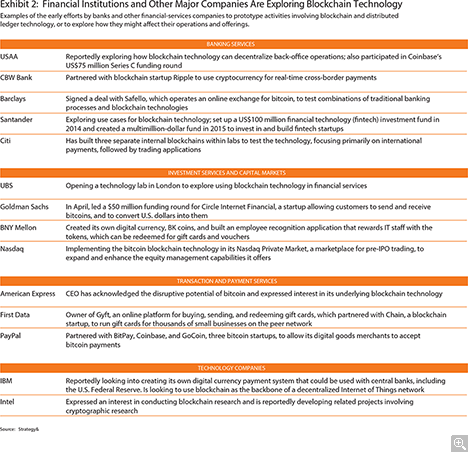


No one is needed to validate its transactions. This is why bitcoin is often referred to as a “trustless” system.

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, 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). 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.

[](http://www.strategy-business.com/media/image/sb82-Blockchain-ex2b.gif)

The technology could also be used to create and support “smart contracts”: code-based, defined sets of rules that sit on top of 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, which can be combined to provide verifiability to any type of transaction. According to the Eris website, the uses could be “as simple as up-voting 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 telephone lines access to communication, information, and electronic 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 receivables 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 options 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 might help 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 Labs 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 its promise. When hiring external consultants and technology providers, choose those who demonstrably understand your company’s strategic direction — not just their own technological 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 measureable, 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.

## Author Profiles:

* [**John Plansky**](mailto: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**](mailto: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**](mailto: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.

## Resources

1. Betsy Burton and David A. Willis, *[Gartner’s Hype Cycles for 2015: Five Megatrends Shift the Computing Landscape](https://www.gartner.com/doc/3111522/gartners-hype-cycles-megatrends-shift" \t "_blank)*, Aug. 12, 2015: Gartner Group predicts that cryptocurrencies will reach a “plateau of productivity” in two to five years.
2. Charity Delich, “[Best of Multimedia: Bitcoin’s Turbulent History](http://www.strategy-business.com/blog/Best-of-Multimedia-Bitcoins-Turbulent-History),” s+b, Mar. 14, 2014: Links to a comprehensive timeline of this technology.
3. Andrew Haldane, “[How Low Can You Go?](http://www.bankofengland.co.uk/publications/Pages/speeches/2015/840.aspx" \t "_blank)” 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.
4. PwC Financial Services Institute, “[Money Is No Object: Understanding the Evolving Cryptocurrency Market](http://www.pwc.com/us/en/financial-services/publications/assets/pwc-cryptocurrency-evolution.pdf" \t "_blank),” PwC, Aug. 2015: Definitive report on cryptocurrency, who is using it, and how it could evolve.
5. Michael Santoli, “[Currency Events](http://www.strategy-business.com/article/00343),” s+b, June 30, 2015: Review of Digital Gold, Nathaniel Popper’s engaging history of bitcoin and related technologies.
6. More thought leadership on this topic: [strategy-business.com/technology](http://www.strategy-business.com/technology)

The Economist

## The blockchain in finance

### Hype springs eternal

# Distributed ledgers are the future, but their advent will be slow

Mar 19th 2016 | [From the print edition](http://www.economist.com/printedition/2016-03-19)

* [imekeeper](http://www.economist.com/news/finance-and-economics/21695068-distributed-ledgers-are-future-their-advent-will-be-slow-hype-springs)

NORMALLY, it is Simon Taylor’s job to persuade sceptical colleagues at Barclays that rapid technological change will disrupt the bank’s business. So it comes as something of a surprise to have to dampen the excitement about the blockchain. “It’s quite silly. I get ten invitations to speak at a conference every day,” he says. “The technology will have real impact, but it will take time.”

The blockchain is the technology underpinning bitcoin, a digital currency with a chequered history. It is an example of a “distributed ledger”: in essence, a database that is maintained not by a single actor, such as a bank, but collaboratively by a number of participants. Their respective computers regularly agree on how to update the database using a “consensus mechanism”, after which the modifications they have settled on are rendered unchangeable with the help of complex cryptography. Once information has been immortalised in this way, it can be used as proof of ownership. The blockchain can also serve as the underpinning for “smart contracts”—programs that automatically execute the promises embedded in a bond, for instance.

It is easy to see why bankers get excited about distributed ledgers. Instead of having to keep track of their assets in separate databases, as financial firms do now, they can share just one. Trades can be settled almost instantly, without the need for lots of intermediaries. As a result, less capital is tied up during a transaction, reducing risk. Such ledgers also make it easier to comply with anti-money-laundering and other regulations, since they provide a record of all past transactions (which is why regulators are so keen on them—see [article](http://www.economist.com/news/business-and-finance/21694968-online-thieves-used-fake-emails-steal-money-101m-bank-heist-unseats" \t "_blank)).

Besides, embracing the technology allows big banks to appear innovative. For the most breathless evangelists, it holds out the prospect of liberation from all the dross that has accumulated in the financial system, from incompatible IT systems to expensive intermediaries. “For many, the blockchain is the Messiah,” says Gideon Greenspan, the founder of Coin Sciences, a blockchain startup based in Israel.

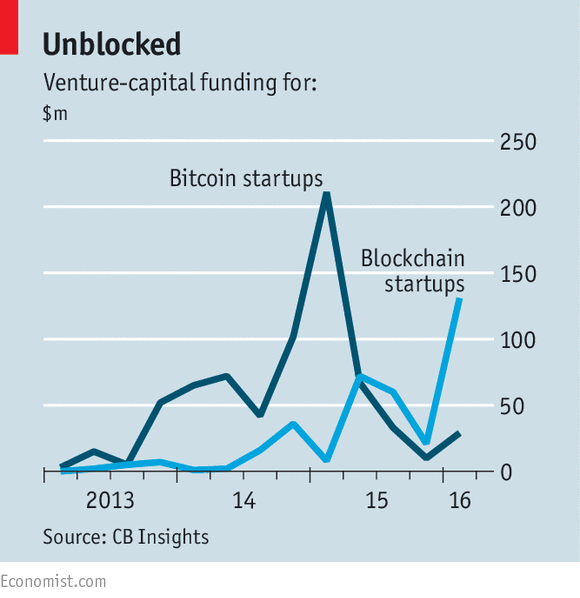
Yet the path to the promised land won’t be an easy one. One stumbling block is what geeks call “scalability”: today’s distributed ledgers cannot handle huge numbers of transactions. Another is confidentiality: encryption techniques that allow distributed ledgers to work while keeping trading patterns, say, private are only now being developed.

Such technical hurdles can be overcome only with a high degree of co-operation between all involved. But this is not a given in the highly competitive world of finance. Some efforts are already under way. More than 40 banks now have a stake in R3 CEV, a startup meant to come up with shared standards. Similarly, firms including IBM and Digital Asset Holdings have started the Open Ledger Project to develop open-source blockchain software.

The Open Ledger Project may have trouble combining the bits of code its members contribute. Such problems will slow adoption, notes Tolga Oguz of McKinsey, a consultancy. Moreover, most projects are still “proofs of concept”. Only a few services have gone live. A dozen banks are using a firm called Ripple to process international payments cheaply. In August Overstock.com, an online retailer, announced a “smart-contract” platform, as did Symbiont, another startup. In January NASDAQ, a stock-exchange operator, launched Linq, a service that allows companies to issue debt and securities. It also plans to initiate a blockchain-based e-voting service for shareholders in firms listed on its exchange in Estonia.

Then there are more specialised services. Everledger uses a blockchain to protect diamonds by sticking data about a stone’s attributes on it, providing proof of its identity should it be stolen. Wave, another blockchain startup, encodes documents used in global supply chains, reducing the risk of disputes and forgeries.

More applications will pop up this year and next. Prime targets will be self-contained markets with complex products, many participants and convoluted procedures. One example is syndicated loans, which can involve dozens of lenders and which can take as long as a month to negotiate. Symbiont recently teamed up with Ipreo, another fintech firm, to automate such loans using smart contracts. Another tempting target is trade finance, which still requires lots of paperwork to travel around the globe along with the goods being sold.



Widespread use of the blockchain is still five to ten years off, predicts Angus Scott of Euroclear, which settles securities transactions. What is more, he says, disruptive fintech startups are unlikely to lead the charge. In markets where the success of a technology depends on its adoption by many counterparties, as is often the case in finance, incumbents have an advantage. The Australian Securities Exchange in January set an example when it enlisted Digital Asset Holdings to develop a blockchain-based system for settling trades.

Given the attenuated timetable and daunting obstacles, there is a risk that banks will lose interest and pursue less glamorous technologies instead. BNY Mellon, an American bank, recently decided not to go ahead with a project that would have used the blockchain to simplify international payments, because it could not persuade enough banks to participate. It would have taken “a significant effort” to make it work, according to Tony Brady of BNY Mellon.

Yet it would be wrong to conclude that the blockchain is no more than a fad. It is merely moving through the same hype cycle as other next-big-things have done before it: inflated expectations are followed by disillusionment before a technology eventually finds its place. Although it will take a while for distributed ledgers to rule the world, they are an idea, to paraphrase Victor Hugo, that will be hard to resist.

NYT

# Bitcoin Start-Up Gets an Electronic Money License in Britain

By [NATHANIEL POPPER](http://topics.nytimes.com/top/reference/timestopics/people/p/nathaniel_popper/index.html)APRIL 6, 2016



A Bitcoin A.T.M. in New York. Circle customers in Britain will now be able to send payments to one another and buy and sell Bitcoin. Credit Danny Ghitis for The New York Times

The British government has pushed through its first licensing of a virtual currency company, underscoring its desire to make London a hub for the development of financial technology.

The Financial Conduct Authority, Britain’s top financial regulator, has granted an electronic money license to Circle, a company based in Boston that uses Bitcoin, the virtual currency, to enable consumers to make payments to other consumers using a mobile app, or “social payments” as the company puts it.

The regulator helped Circle get the license by putting it in the government’s Innovation Hub, which is one of several initiatives Britain has undertaken to encourage experimentation in the financial industry.

The license makes it possible for Circle to establish a banking relationship with [Barclays](http://www.nytimes.com/topic/company/barclays-plc?inline=nyt-org), the British bank. It is the first time that a large global bank has agreed to work with a Bitcoin company, [though Circle has attracted investments from others](http://www.nytimes.com/2015/04/30/business/dealbook/goldman-and-idg-put-50-million-to-work-in-a-bitcoin-company.html).

The British economic secretary to the treasury, Harriett Baldwin, said in an email that the license and Barclays’ relationship with Circle “prove our decision to introduce the most progressive, forward-looking regulatory regime is paying off and cements our status as the world’s fintech capital.”

Circle, which was founded in 2013, already allows customers in the United States to easily send payments to one another and buy and sell Bitcoin, and customers in Britain will now be able to do the same.

But Circle has long aimed to use Bitcoin as a back-end network to make it easier and cheaper to move money between national currencies. The Bitcoin technology, which first emerged in 2009, has been promoted as a way to quickly and cheaply move money across national borders without using traditional money-transmitting services such as Western Union.

Circle is set up so that its customers can hold their money in national currencies to avoid the volatile price of Bitcoin. When a customer wants to move money, he or she can buy Bitcoin for the short period of time required to send the money or simply move dollars or pounds from a linked bank account.

Photo



Jeremy Allaire of Circle says consumers “will be able to beam sterling and dollars back and forth, instantly for free.” Credit Gretchen Ertl for The New York Times

The British license will allow Circle customers to instantly transfer money between dollars and British pounds — and soon enough, between those currencies and euros, given that the e-money license is valid across the European Union.

“For the first time any consumer in the U.S. and the U.K. will be able to beam sterling and dollars back and forth, instantly for free,” said Jeremy Allaire, the co-founder of Circle. “That’s just never been possible.”

It is a difficult moment for the virtual currency. The developers who maintain the basic Bitcoin software have been divided over updates to the software. That has caused a [schism in the Bitcoin community](http://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables-transactions-that-rival-bitcoins.html) and slowed down transactions.

Some companies [have been looking at other virtual currencies, such as Ethereum](http://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables-transactions-that-rival-bitcoins.html), as an alternative way to transfer money using what is known as a blockchain, the database concept that Bitcoin introduced. Mr. Allaire said that Ethereum was not yet ready for global use in the same way as Bitcoin, but that it could be in the future.

“We are not wedded to one blockchain as the right one,” he said.

In the United States, Circle has not managed to take Bitcoin mainstream, but it has gotten Bitcoin some key seals of approval. Back in 2013, it got funding from the major venture capital firms Accel Partners and General Catalyst Partners. And last year, Circle became the first company to get a so-called BitLicense from New York state’s top financial regulator, the Department of Financial Services.

The New York agency had been the only regulatory body to devise a licensing system for virtual currency companies, trying to confront the fraud and crime that have plagued the technology.

But the British government has taken several steps to emphasize its interest in attracting virtual currency start-ups, among other types of financial technology, to London.

The British chancellor of the Exchequer, George Osborne, [publicly purchased virtual currency from a Bitcoin A.T.M. in 2014](http://www.coindesk.com/george-osborne-unveils-uk-plans-explore-bitcoin/) at an event where he announced the government’s desire to work with virtual currency companies.

The moves appear to be, at least in part, a way to draw new businesses to London as many parts of the financial industry have struggled with lagging revenue.

Several executives at Barclays have [previously discussed the bank’s interest in Bitcoin](http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html) and the blockchain technology. The [bank has labs in London dedicated to experimenting](http://www.businessinsider.com/barclays-derek-white-on-bitcoin-and-blockchain-2015-9?r=UK&IR=T) with the technology.

Computerworld

# IBM offers advice on how to secure blockchain in the cloud

Credit: [Deavmi](https://commons.wikimedia.org/wiki/User:Deavmi" \t "_blank)

## The company wants to drive broad blockchain adoption, but also bring users to its cloud services

[](http://www.computerworld.com/author/Grant-Gross/)By [Grant Gross](http://www.computerworld.com/author/Grant-Gross/)

[Follow](http://www.computerworld.com/article/3062921/security/ibm-offers-advice-on-how-to-secure-blockchain-in-the-cloud.html?token=%23tk.CTWNLE_nlt_computerworld_security_2016-05-02&idg_eid=388c00fe17899e0b331bde0fdc894ad9&utm_source=Sailthru&utm_medium=email&utm_campaign=Computerworld%20Security%202016-05-02&utm_term=computerworld_security#follow)

[IDG News Service](http://www.idgnews.net/" \t "new) | Apr 29, 2016 10:33 AM PT

Cloud providers hosting blockchain secure transactions technology should take additional steps to protect their records, IBM says.

IBM's [new framework](http://www.ibm.com/blockchain/how_can_ibm_help.html" \t "new) for securely operating blockchain networks, released Friday, recommends that network operators make it easy to audit their operating environments and use optimized accelerators for hashing -- the generation of numbers from strings of text -- and the creation of digital signatures to pump up CPU performance.

Along with the security guidelines, IBM announced new cloud-based blockchain services designed to meet existing regulatory and security requirements. The company has worked with security experts to create cloud services for "tamper-resistant" blockchain networks, it said.

The new cloud services are "an iron-clad way to achieve that level of security," said Holli Haswell, an IBM spokeswoman. "Not all clouds can necessarily attain that level of security and compliance today."

While blockchain, traditionally used for bitcoin and other financial transactions, is already focused on security, most businesses will need to use blockchain in permission-based networks shared on the cloud, Haswell said by email.

"You don’t want bad actors like a VM (virtual machine) manager in the host provider to see when transactions are coming in or trying to perform interrogations that could give them sensitive information," she added.

Network operators should also protect their blockchain operating environments from access by host administrators to prevent tampering, recommended IBM, which has embraced blockchain technology in recent months.

Haswell described the IBM framework as "a set of standards or recommendations that we believe should be adhered to or at least considered when putting blockchain applications in the cloud once they move from experiments to production environments."

IBM in February [announced](http://www.computerworld.com/article/3033919/security/ibm-pushes-ahead-on-blockchain-offers-cloud-based-service.html) it is offering a cloud-based service to allow developers to set up blockchain networks and test and deploy related apps.

Blockchains are distributed records of events, each block in the record containing a computational "hash" (or numeric representation) of itself and of the previous block, like links in a chain. Blockchains make it difficult to modify or fake past transactions because such a change would require the modifications to be made on all subsequent blocks.

IBM is [pitching](http://www-03.ibm.com/press/us/en/pressrelease/49632.wss" \t "new) its own secure blockchain services at financial services companies, government agencies and healthcare firms, the company said. But other cloud providers can adopt the company's new blockchain security framework, Haswell noted.

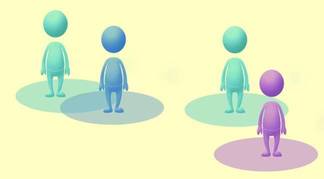
The company hopes the security guidelines will help drive adoption of blockchain, she said. The guidelines will help providers scale to thousands of users securely, she added.

**Institute for the Future**

## Game Room: Blockchain Meets Virtual Reality

**May 10, 2016** By [Kathi Vian](http://www.iftf.org/kathivian/)

In 2010, IFTF’s [Ten-Year Forecast](http://www.iftf.org/our-work/global-landscape/ten-year-forecast/2010-ten-year-forecast/) suggested that the future is a high-resolution game:

**"Never before has humanity been able to encounter the future in such detail, to measure the forces of change at such vast scales, and to fill in the details with such fine grain. As we play this game, we find ourselves in ever more layered and nuanced futures that often look distinctly different across geographies, across cultures, and even across the various identities each of us claims.**

**More than a fragmented marketplace or a contentious body politic, this future looks like a massively branching game environment where you can win without ever discovering half of the possible pathways—but you can lose by mistaking a clear line of sight for the whole story."**

As we try to grasp the future of blockchain and other distributed computing technologies, we have to start here, with this high-resolution gamescape where there is no single blockchain future. Rather, we face an ecosystem of futures as complex as the global superorganism that we are actually becoming. We mustn’t forget that as blockchain technology unfolds into financial, legal, environmental, and biological realities, it will blend with other high-resolution technologies to change every assumption we have about what’s possible in the economy, in human society, and even the biological world.

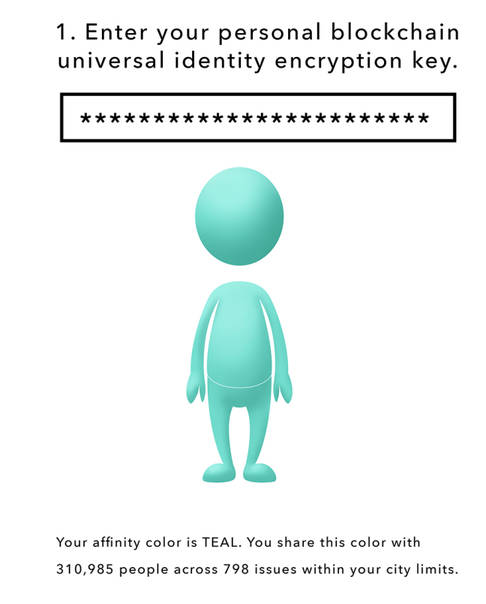
It will amplify and be amplified by a rapidly emerging capacity for high-res virtual reality simulations and games. The Internet of Things, including the Internet of Living Things, will create a highly distributed grid across which blockchain transactions of all kinds are negotiated by learning algorithms and executed by smart contracts. These transactions will, of course, be verifiable by millions, maybe billions of mobile computing devices. Biological programming—editing the individual genes of individual cells for specific functions—will open a vast and contentious landscape of biological transactions to be provisioned, regulated, and supported by blockchain architectures.

Even as companies and consortia are trying to discover the core application zones for this new distributed computing technology, we need to look ahead to unexpected intersections of high-res technologies if we really intend to see the array of unexpected scenarios that lie in wait in the high-resolution blockchain future.

For example, for the most recent Ten-Year Forecast, entitled “[The Future Is a Rite of Passage](http://www.iftf.org/iftf-you/programs-initiatives/ten-year-forecast/),” we posited a Virtual City Council. We were inspired by [Pia Mancini’s Democracy OS](http://democracyos.org/" \t "_blank), which ultimately imagines a digital platform for global citizenship. But we decided to start local with what we called “governance in your game room.”

This scenario brings citizenship into your 2030 virtual 3D game room and integrates it into everyday choices of what you eat, what you buy, and how you play. But unlike [China’s controversial 2020 citizen scoring proposal](https://en.wikipedia.org/wiki/Social_Credit_System" \t "_blank), the Virtual City Council is not a top-down centralized social or citizenship scoring system. Rather it’s a bottom-up distributed toolset for aggregating large groups of people with similar interests, needs, and values into civic affinity groups. Where individual preferences and priorities might otherwise get lost in the fragmented consumer landscape of targeted advertising, they now form the basis for connecting like-minded people across citizenship issues ranging from health and food to safety in public spaces.

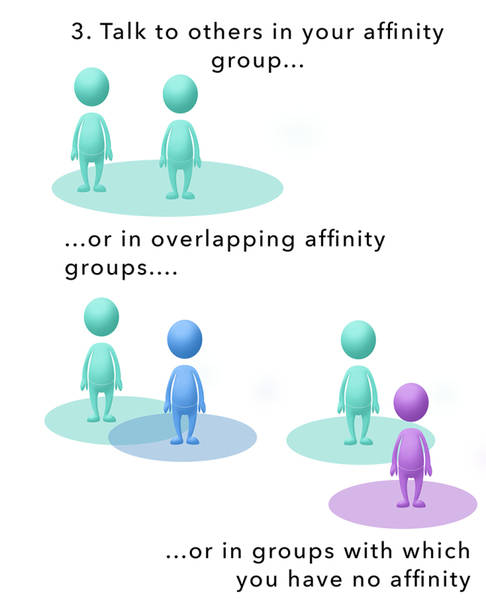
You start by granting anonymous access to your encrypted transaction records across the many blockchains you use in your daily life. Without revealing your actual identity, you can tap the intelligence of virtual digital assistants and learning algorithms to discover the issues that are most important to you.



Your virtual immersive reality represents these affinity groups as spotlights in 3D space. You move from spotlight to spotlight to discover your affinity groups.



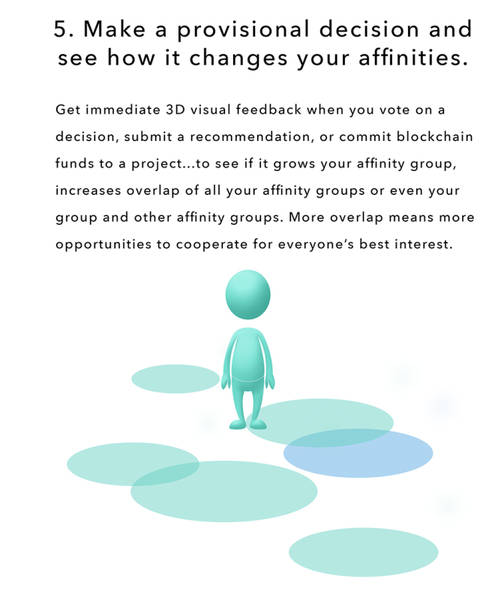
This virtual city council is not simply passive profiling, however. You can interact with others to explore the issues with people who are a lot like you, a little like you, or very different from you. These interactions create the opportunities to develop more nuanced affinities with large numbers of people.



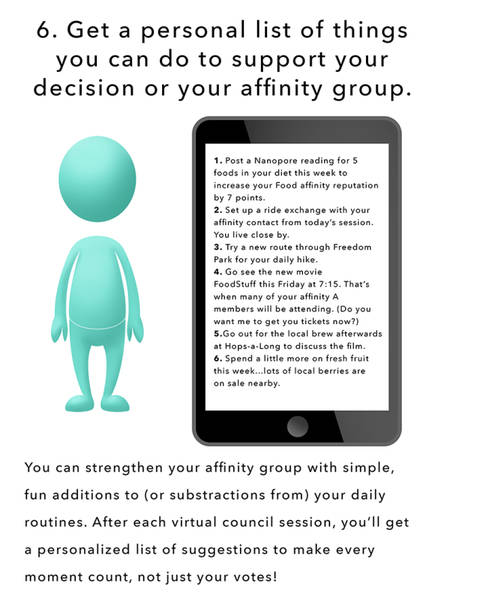
You might also draw on your personal virtual representative to learn more about issues that often have seemingly intractable dilemmas at their core. Behind this virtual representative, we might well find a set of optimization algorithms that look the best solutions for the range of citizens.



In this world of game room governance, you can test your decisions or votes or donations to see how they change your affinities—and ultimately grow or diminish your influence. In other words, your virtual city council provides immediate feedback loops to help you refine your decisions and personal actions.



And speaking of personal actions, you can even get a “to-do” list of activities that can strengthen your affinity group culture.



This scenario is not a prescription for the future. It’s simply a provocation for thinking about what’s possible when blockchain tools intersect other high-resolution technologies on the not-so-distant horizon. It shows us a way that entirely new identities, including collective identities, might emerge over the next decade. It shows how the affordances of transparency and pseudonymity might actually build more cohesive and functional societies from very high-resolution transactions.

Ultimately, it calls on us to think beyond the next killer blockchain app to imagine the different kinds of worlds we’ll find ourselves building as distributed computing defines the next era of digital society.

* + See more at:

<http://www.iftf.org/future-now/article-detail/game-room-blockchain-meets-virtual-reality/#sthash.ll23Hv2y.dpuf>

Yahoo Finance

# Here's where big banks stand on blockchain

## An inside view from the authors of "Blockchain Revolution"

Video @ [http://finance.yahoo.com/news/here-is-what-wall-street-and-big-banks-think-about-blockchain-where-they-stand-tapscott-bitcoin-book-040128769.html#](http://finance.yahoo.com/news/here-is-what-wall-street-and-big-banks-think-about-blockchain-where-they-stand-tapscott-bitcoin-book-040128769.html)

In case you haven’t heard, [blockchain is all the rage lately on Wall Street](http://finance.yahoo.com/news/big-banks-interest-in-blockchain-r3-052723646.html?soc_src=mediacontentstory&soc_trk=tw), whereas bitcoin, the digital currency that blockchain came along with in 2009, is suddenly very uncool.

Blockchain, by the way, is the decentralized, peer-to-peer, open-source, distributed ledger technology that underlies bitcoin. (Check out our [video explainer on blockchain](http://finance.yahoo.com/news/the-biggest-bitcoin-and-blockchain-news-announcements-at-consensus-conference-2016-chain-21-delaware-craig-wright-032242815.html).) The bitcoin blockchain is just one use case of the technology; lately the idea of utilizing the same technology, apart from cryptocurrency, has become popular. **As Bloomberg’s Matt Levine wrote earlier this month, “If you are any sort of self-respecting financial or finance-adjacent professional these days,** [**you had better be inserting the word ‘blockchain’ into random sentences**](http://www.bloomberg.com/view/articles/2016-05-02/interrogation-methods-and-blockchains) **to prove that you're up to speed.”**

Indeed, banks and financial services have certainly hopped aboard the blockchain train. But behind public press releases about initiatives and blockchain experimentation, executives at these companies differ greatly in their thinking on the technology and their faith in it.

Father-and-son team Don and Alex Tapscott, both business strategy consultants, have a new book out today called “Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World.” A more apt title might hedge that the technology “could” change the world, but the book makes a convincing case for why blockchains might revolutionize the financial sector. (And many other sectors, but for now, the excitement is starting with finance.) For their research, the Tapscotts spoke to numerous people in banking.

Alex Tapscott says people in banking fall into four categories right now in their attitudes about blockchain. It’s worth including here his full explanation, as told to Yahoo Finance:

“There are still a few who are generally afraid of this or don’t fully buy into it, but are trying to learn more. That’s increasingly a minority. More people these days fall into a second category, which is they see this as an opportunity to reduce cost in their existing business. That’s interesting. But for us, the bigger opportunity, and I think increasingly more financial services firms fit into this, is to say, How can we use this new technology platform to fundamentally reinvent our business? If billions of people in the world don’t have access to financial services, maybe we can be the ones to harness this new technology to offer them the same services we offer our existing clients. Now, there’s a fourth category of course: if you’re a bank that thinks this is all nonsense, I would highly recommend you at least upgrade to fearful. Because this change is happening.”

Well, blockchain believers may say the change is happening. And there are signs that is the case. To cite just two examples: [More than 45 banks have signed on to blockchain consortium R3 CEV](http://finance.yahoo.com/news/big-banks-interest-in-blockchain-r3-052723646.html?soc_src=mediacontentstory&soc_trk=tw), including Goldman Sachs ([GS](http://finance.yahoo.com/news/finance.yahoo.com/q?s=GS" \t "_blank)), JPMorgan ([JPM](http://finance.yahoo.com/news/finance.yahoo.com/q?s=jpm" \t "_blank)), and Bank of America ([BAC](http://finance.yahoo.com/news/finance.yahoo.com/q?s=bac" \t "_blank)), to test out blockchain tech for their transaction-settling processes; and [blockchain startup Chain recently announced it had completed a blockchain-for-banking product](http://finance.yahoo.com/news/the-biggest-bitcoin-and-blockchain-news-announcements-at-consensus-conference-2016-chain-21-delaware-craig-wright-032242815.html) and revealed Citi ([C](http://finance.yahoo.com/news/finance.yahoo.com/q?s=C" \t "_blank)), Visa ([V](http://finance.yahoo.com/news/finance.yahoo.com/q?s=v" \t "_blank)), and other heavy-hitters as launch partners.

But bitcoin believers (and yes, there are still many) say that [the concept of closed, permissioned blockchains, without digital currency, doesn’t make much sense](http://finance.yahoo.com/news/how-early-bitcoin-company-coinbase-adapting-to-blockchain-frenzy-fred-ehrsam-brian-armstrong-bitcoin-exchanges-140054770.html). At most, bitcoin executives say, it can improve back-office I.T. functions of banks, which is a rather unsexy proposition for a technology that can do much more. Some are hopeful that blockchains can eventually deliver a decentralized form of all kinds of technology platforms, including, say, Uber. “It’s the disruptors themselves that stand to be disrupted,” Alex Tapscott says, describing the possibility of a "super Uber" that cuts out the middleman operator.

As Don Tapscott explains, banks should be thinking bigger than they are. They ought to be aiming to revamp their systems entirely, rather than simply to improve efficiencies and reduce costs. “The blockchain is the biggest innovation in computer science in a generation, we think," he says. "And what it represents is the Internet of value. We’ve had the Internet of information for several decades. But when it comes to exchanging value—not just money, but music or loyalty points or stocks or bonds—you can’t do that in a peer-to-peer way without a powerful intermediary. This has resulted in a situation where powerful intermediaries are capturing all the value of the digital age."

That phrase, the "Internet of value," or something very close to it, has been used before to describe bitcoin and the blockchain. In fact, [it’s the subject of an ongoing dispute between a prominent “cloud money” startup and an equally prominent figurehead within the bitcoin community](http://finance.yahoo.com/news/bitcoin-world-disputes-uphold-internet-of-money-andreas-antonopoulos-210907255.html). The latter, Andreas Antonopoulos, argues that “Internet of Money” is the best phrase to describe the promise of bitcoin, and that no one company ought to be using it as a corporate slogan.

Balaji Srinivasan, a partner at mega-influential VC firm Andreessen Horowitz and the CEO of bitcoin software company 21.co, has a similar idea for bitcoin, and is skeptical of the “blockchain minus bitcoin” fad. His vision: [To create a “machine economy” in which computers can pay each other seamlessly](http://finance.yahoo.com/news/why-21-inc-is-the-most-exciting-bitcoin-blockchain-company-balaji-srinivasan-andreessen-horowitz-200250565.html) in bitcoin.

As the Tapscotts do make clear in their book, we are still in the early days of this space. It is so early, in fact, that much of the mainstream media only covers this industry when there are salacious new reports of [who might be the real Satoshi Nakamoto, the creator of bitcoin](http://finance.yahoo.com/news/australian-craig-wright-admits-creating-bitcoin-but-satoshi-nakamoto-identity-does-not-matter-152400952.html). They are missing what is really going on here, but they still have ample time. In the simultaneous races to innovate in both bitcoin and blockchain, there is not yet any clear victor.

The Blockchain Revolution is available now. Watch the above video for a more in-depth discussion about the book with its authors.

K@W

#### [Finance](http://knowledge.wharton.upenn.edu/topic/finance/)

# How Blockchain Technology Will Disrupt Financial Services Firms

May 24, 2016

* [Global Focus](http://knowledge.wharton.upenn.edu/region/global-focus/)
* [North America](http://knowledge.wharton.upenn.edu/region/north-america/)





In the second article of the [*series*](http://knowledge.wharton.upenn.edu/article/the-network-revolution-creating-value-through-platforms-people-and-digital-technology/), “The Network Revolution: Creating Value through Platforms, People and Technology,” authors [*Barry Libert*](https://www.linkedin.com/in/barrylibert), [*Megan Beck*](https://www.linkedin.com/in/meganbeck) and [*Jerry (Yoram) Wind*](https://marketing.wharton.upenn.edu/profile/196/) look at how blockchain technology will prove to be a major disruptor to the public and private sectors, starting with the financial services industry. Libert is CEO of OpenMatters and Beck is the chief insights officer. Wind is a Wharton marketing professor and director of Wharton’s SEI Center for Advanced Studies in Management. The authors would like to thank [*LiquidHub*](http://www.liquidhub.com/) for sponsoring the research for this series.

\* \* \*

“There are hundreds of startups with a lot of brains and money working on various alternatives to traditional banking.” — Jamie Dimon, JPMorgan Chase

The basic rules of the game for creating and capturing economic value were once fixed in place. For years, or even decades, companies pursued the same old business models (usually selling goods or services, building and renting assets and land, and offering people’s time as services) and tried to execute better than their competitors did. But now, business model disruption is changing the very nature of economic returns and industry definitions. All industries are seeing rapid displacement, disruption, and, in extreme cases, outright destruction. The financial services industry, with its large commercial and investment banks and money managers, is no exception.

“Silicon Valley is coming,” [JPMorgan Chase CEO Jamie Dimon warned in his annual letter to shareholders](http://files.shareholder.com/downloads/ONE/15660259x0x820077/8af78e45-1d81-4363-931c-439d04312ebc/JPMC-AR2014-LetterToShareholders.pdf). He said startups are coming for Wall Street, innovating and creating efficiency in areas that are important to companies such as JPMorgan, particularly in the lending and payments space.

The payments startup Stripe has a multibillion-dollar valuation and a partnership with Apple Pay. Bitcoin companies and exchanges such as 21 and Coinbase are attracting tens of millions of dollars from venture capitalists. Peer-to-peer lending is booming in the small loan market with many players, including Upstart, Prosper, Funding Circle, and more. And the financial-planning startup [LearnVest just got acquired for more than $250 million.](http://www.businessinsider.com/northwestern-mutual-acquires-learnvest-2015-3)

Many of these organizations are in the lending business, but are using big data and cloud technologies rather than tellers and branches to speed lending and customer acquisition. Others are leveraging network business models, such as peer-to-peer lending, to bring together would-be lenders and borrowers. According to Dimon, “We are going to work hard to make our services as seamless and competitive as theirs.” His underlying thought is this: If his company doesn’t keep pace with today’s well-capitalized upstarts, they will begin to lose relevance in a platform-centric world.

“In lots of areas, it looks like the blockchain will replace the current centralized business model of the financial services industry.”

There are many innovative, network business models that are coming after traditional financial services and banking organizations, and big banks are beginning to realize they must evolve in response if they want to remain viable in a digitally centric world — whether it comes by acquiring, partnering or developing leading-edge technologies. But what’s less clear is why, exactly, these new entrants are so disruptive and powerful. What enables them to skirt perceived constraints of these once ‘too large to fail’ incumbents and exploit unseen possibilities? In short, it is network-centered thinking with platform-based business models.

#### Sponsored Content:

**Control Shifting Away from Central Banks**

In London’s Canary Wharf, a team of technologists and executives are trying to understand how to use blockchain technology to change the future of banking globally. Their leader is Blythe Masters, an ex-Wall Street commodities trader turned digital entrepreneur focused on turning the mental model and business model of the massive financial services industry and all its related parties (consumers, lawyers, accountants) on its head.

Bank executives worldwide are trying to figure out what this evolution in technology will mean for their firms. “We could go the way that file transfer technology changed music, allowing new businesses like iTunes to emerge. That is why there is such feverish activity at the moment,” said Michael Harte, chief operations and technology officer at Barclays, according to a recent article in The Financial Times.

For the massive financial services sector, blockchain technology (the software behind the digital currency, Bitcoin) offers an opportunity to overhaul its existing business model, including its banking infrastructure, approach to settlements and customer interactions. But acting on this opportunity, and making the most of the blockchain, is no easy task given the core beliefs and reinforcing systems that are embedded in the industry.

**Networks Are Taking Over**

What is the blockchain? It is a distributed database of computers that maintains records and manages transactions. Rather than having a central authority (such as a bank), blockchain uses the network to approve “blocks,” or transactions, which are then added to the “chain” of computer code.  Cryptography is used to keep transactions secure, and the distributed nature of transaction approval makes the system harder to tamper with.

“It is only a matter of time before the broader financial services and banking industries shift to blockchain and network-based approaches.”

Blockchain technology has been hailed by its VC supporters as having revolutionary promise for all involved. “You should be taking this technology as seriously as you should have been taking the development of the Internet in the early 1990’s. It’s analogous to email for money,” said Masters, according to The Financial Times.

And blockchain enthusiasts believe that the application possibilities are endless — improving the way we hold and transfer secure goods from money to deeds to music to intellectual property. In fact, blockchain, as a pure platform technology, may be able to cut out the middlemen (or middle companies) everywhere, even disrupting other disruptors like Airbnb or Uber.

In the present financial services business model, a central ledger most often acts as the custodian of that information (such as the Federal Reserve and its member banks). But in a blockchain world, the information regarding each transaction is transparently held in a digitally shared database in the cloud, without a single central body acting as the middleman. This lack of central authority is the very feature that is turning the current mental and business models of traditional financial institutions on their heads.

In a lot of areas, it looks like the blockchain will replace the current centralized business model of the financial services industry and it is easy to see how it could revolutionize all of Wall Street. The ability of the technology to provide an unforgeable record of identity, including the history of an individual’s transactions, is one area being eagerly explored. David Grace, head of global finance at PwC, said that “if you have a secure distributed ledger, it could be used to store validated ‘know your customer’ data on individuals or companies. … It’s a potentially global application that could provide more security over identity data and where that data are stored.”

“It seems that the code can perform better than a real middleman in most cases.”

Clearly, we are entering a period of rapid evolution, as the financial services industry determines blockchain and what it means for their business models. Or, another scenario: A slew of startups identifies the possibilities and pulls the rug out from under big institutions. Traditional perceptions about the roles of financial players are already under attack — as it seems that the code can perform better than a real middleman in most cases. Old business models will soon fall prey to the quickly evolving technology and mental models. The network is about to do its magic: Grow and evolve without central control.

**Network Business Models Will Dominate**

Blockchain is already seeing use outside of the financial services sector, where it got its start. Technology and services giant IBM is adapting the blockchain methodology to develop a currency-less system that could be used for any purpose — for example, executing contracts upon delivery.

Arvind Krishna, senior vice president of IBM Research, believes that in the long run, this technology could facilitate transactions between banks or international businesses. “I want to extend banking to the 3.2 billion people who are going to come into the middle class over the next 15 years,” he said. “So I need a much lower cost of keeping a ledger. Blockchain offers some intriguing possibilities there.” A firm-centered or centrally controlled banking system clearly will not get him there, and the blockchain will allow him to leverage a digitally-enabled network as the way forward.

**Join the Network Revolution**

With companies such as IBM and JPMorgan Chase, as well as preeminent venture capitalist firm Andreessen Horowitz, backing this new way of facilitating financial transactions, [it is only a matter of time before the broader financial services and banking industries shift to blockchain and network-based approaches](https://twitter.com/intent/tweet?original_referer=http%3A%2F%2Fknowledge.wharton.upenn.edu%2Farticle%2Fblockchain-technology-will-disrupt-financial-services-firms%2F&url=http%3A%2F%2Fknlg.net%2F1TvJBSm&source=tweetbutton&text=Financial%20services%20firms%20will%20be%20shifting%20to%20blockchain%2C%20network-based%20approaches%20%40whartonknows%20%40jerrywind" \t "_blank)*[Twitter](https://twitter.com/intent/tweet?original_referer=http%3A%2F%2Fknowledge.wharton.upenn.edu%2Farticle%2Fblockchain-technology-will-disrupt-financial-services-firms%2F&url=http%3A%2F%2Fknlg.net%2F1TvJBSm&source=tweetbutton&text=Financial%20services%20firms%20will%20be%20shifting%20to%20blockchain%2C%20network-based%20approaches%20%40whartonknows%20%40jerrywind" \t "_blank)* to complement, or replace, the current centralized approach. The question is not whether network business models supported by blockchain technology will disrupt these organizations, but when. So if you are a member of the current financial services industry elite — or a local bank or credit union — it’s time to become part of the digital revolution and join the network and platform-emerging world.

Fortune

# What Wall Street’s Obsession With Blockchain Means for the Future of Banking

* COMMENTARY by
* [Howard Yu](http://fortune.com/author/howard-yu/)
* [@HowardHYu](https://twitter.com/HowardHYu" \t "_blank)

July 10, 2016, 9:00 PM EDT



**And your wallet**

Howard Yu is professor of strategic management and innovation at IMD. He specializes in technological innovation, strategic transformation and change management. In 2015 Professor Yu was featured in Poets & Quants as one of the Best 40 Under 40 Professors. He received his doctoral degree at Harvard Business School.

Anyone who sends money abroad knows how inconvenient it is. Banks take days, sometimes weeks, to clear payments, and they collect a [hefty fee](http://www.nbcnews.com/business/new-rule-protects-those-who-make-international-wire-transfers-8C11466340" \t "_blank) in between. And God forbid, when errors occur, money [vanishes](http://www.thisismoney.co.uk/money/saving/article-2188381/My-7-000-just-vanished-How-slip-finger-cost-life-savings.html" \t "_blank) into thin air. “Banking now is like sending a letter—you send it [and] you don’t know if it reached [its destination],” [observed Chris Larsen](http://www.cnbc.com/2016/06/22/banks-trial-ripple-blockchain-to-make-international-money-transfers-like-sending-an-imessage.html" \t "_blank), CEO and co-founder of Ripple, a San Francisco-based startup. His vision is simple: Money transfer should be like sending an iMessage, where you immediately know if and when it arrives. It’s a bold, disruptive idea for sure, but it’s a vision eagerly embraced by heavyweights on Wall Street.

Just last month, [IBM](http://fortune.com/fortune500/ibm-31/" \t "_blank) [IBM](http://fortune.com/fortune500/ibm-31/) 0.82% and Crédit Mutuel Arkéa announced the completion of their [first blockchain project](http://www-03.ibm.com/press/us/en/pressrelease/50087.wss" \t "_blank). The week before, a group of [seven banks](http://fortune.com/2016/06/23/ripple-blockchain-banks/" \t "_blank), including UBS [UBS](http://fortune.com/company/ubs/) 2.20% , Santander [SAN](http://fortune.com/company/san/) 1.92% , and UniCredit, were trying to move money across borders using a blockchain platform that Ripple created. [Goldman Sachs](http://fortune.com/fortune500/goldman-sachs-group-74/" \t "_blank) [GS](http://fortune.com/fortune500/goldman-sachs-group-74/) 1.28% and Barclays [BCS](http://fortune.com/company/bcs/) 4.51% had similarly invested in yet [another venture](http://www.reuters.com/article/us-bank-payment-circle-idUSKCN0X30A7" \t "_blank), aiming to make real-time money transfer possible. Even [JPMorgan Chase](http://fortune.com/fortune500/jpmorgan-chase-23/" \t "_blank) [JPM](http://fortune.com/fortune500/jpmorgan-chase-23/) 1.21% , an initial blockchain [skeptic](http://fortune.com/2015/11/04/jamie-dimon-virtual-currency-bitcoin/" \t "_blank), has now joined [Citigroup](http://fortune.com/fortune500/citigroup-29/" \t "_blank) [C](http://fortune.com/fortune500/citigroup-29/) 1.57% , [Bank of America](http://fortune.com/fortune500/bank-of-america-corp-26/" \t "_blank) [BAC](http://fortune.com/fortune500/bank-of-america-corp-26/) 1.33% , and Credit Suisse [CS](http://fortune.com/company/cs/) 2.29% to test out application in the [credit derivatives market](http://www.wsj.com/articles/bitcoins-blockchain-technology-proves-itself-in-wall-street-test-1460021421" \t "_blank). Blockchain, a record-keeping technology that powers Bitcoin—the first digital currency—has irrevocably gone mainstream.

Until most recently, Bitcoin was infamously associated with drug dealers, pornography, and the illicit weapons trade. To possess the kind of eagerness Wall Street has in experimenting with blockchain is like Sony Music Entertainment [SNE](http://fortune.com/company/sne/) 1.90% or Warner Music Group dabbling in peer-to-peer music sharing when Napster was at its height in the late ’90s. Little wonder that some observers likened blockchain to an unregulated open field. Jamie Smith, former spokesperson for President Obama, argued for the need to engage policy makers more widely, calling [educating regulators](http://www.coindesk.com/how-to-get-the-upper-hand-on-regulatory-policy/" \t "_blank) a top priority.

In short order, an unlikely [alliance was forged](http://www.coindesk.com/bitcoin-groups-and-law-enforcement-unite-to-form-blockchain-alliance/" \t "_blank). Startups with names that have barely entered the public conscious (e.g. BitFury, BitGo, Bitnet, Bitstamp, itBit) are now working with the U.S. Justice Department, the FBI, and the Commodity Futures Trading Commission. Still, the most ardent supporters of blockchain came not from Silicon Valley, but from Wall Street. Unlike major music labels who ignored, shunned, and deplored peer-to-peer file sharing, the pinstripe suit–wearing bankers suddenly turned into adventurous entrepreneurs. What changed this time?

Every intricacy of modern banking is an attempt to answer a fundamental question posed by capitalism: How do we get strangers to trust one another? Let’s say Mary, a mother living in New York, wants to wire $1,000 to her son, David, who is studying abroad in Madrid. Upon order, the U.S. bank immediately debits Mary’s account and puts the money on hold at the Federal Reserve, which waits to aggregate hundreds of thousands of daily transactions before sending them in a batch to the European Central Bank. The European Central Bank then dispatches the bundle and schedules the distribution of individual transactions to different local banks. After two to four days, David finds the equivalent of $900 appearing in his local account after the deduction of about 10% in administrative and exchange fees charged by every intermediary in the chain.

This maddening system isn’t that different from the original banking system invented more than a century ago. The advantage? Along this great chain of being, everyone needs to talk only to someone they trust. U.S. banks talk only to the Federal Reserve, the Federal Reserve talks only to the European Central Bank, and so on.

The last time some real innovation occurred was in 1871, when Western Union—a telegraph company—introduced a proprietary system that achieves near real-time money transfer. With 500,000 points of sale scattered around the world, [Western Union](http://fortune.com/fortune500/western-union-468/" \t "_blank) [WU](http://fortune.com/fortune500/western-union-468/) 0.36% allows Mary to bring cash to its counter, and in a few minutes, David can withdraw cash from another Western Union across the Atlantic. No more talking to multiple parties. This system requires massive scale, and it’s expensive, but it works. [PayPal](http://fortune.com/fortune500/paypal-holdings-307/" \t "_blank) [PYPL](http://fortune.com/fortune500/paypal-holdings-307/) 1.20% , in many ways, is simply the online version of the same ingenious design.

Now imagine a world where the identity of the account holder is masked, but everyone can see the money in every account. In other words, everyone owns the same ledger, and it can’t be easily altered unless you can gain control of the majority of all of the computing resources. When Mary’s money is deducted and David’s is added, the movement is completely transparent, so no reconciliations or double-checking is needed between multiple parties. The system is designed to be real time—instantaneous. Such is the basic logic of Bitcoin, and its technology blockchain—an open ledger that all can see effectively cuts out the need for central banking oversight.

Blockchain, it turns out, is just a universal banking protocol—a big idea to be sure, much like the Internet protocol that ushered in the World Wide Web. Everything blockchain needs is already here, from mobile phones to embedded sensors, from raw computing power to machine algorithms. The greatest achievement of Satoshi Nakamoto, the mysterious inventor of Bitcoin, is to commit such an elegant design of a decentralized monetary system to paper that it inspired waves of hackers, technologists, and bankers to experiment in a number of different ways.

The enthusiasm of big banks is understandable. The regulatory pressure to record everything from stock trades to money transfer has caused compliance costs to escalate astronomically in recent years. From Basel III (509 pages including 78 calculus equations) to the Dodd-Frank Act (2,300 pages), our centralized system reeks of Soviet-style command and control. Just by eliminating the manual processes around reconciliation with customers, trading partners, and securities exchanges, it has been estimated that blockchain will deliver savings of nearly [$20 billion](http://www.fastcompany.com/3059425/how-banks-learned-to-stop-worrying-and-love-the-blockchain-bitcoins-underlying-tech" \t "_blank) per year by 2022—net profit straight to the bottom line.

This is why big banks are scrambling to explore new applications, such as unforgeable records of identity, to achieve straight-through processing, with transactions automated completely with no human intervention. Greenwich Associates, a market intelligence provider, reported in a survey that financial and technology markets will invest [$1 billion](https://www.cryptocoinsnews.com/financial-and-technology-sectors-to-invest-1-billion-in-blockchain-technology-in-2016/" \t "_blank) in blockchain this year.

But doesn’t Wall Street care about job security? Not when it directly boosts the bottom line. When savings are tangible, big companies are willing to soldier through any wrenching change. American manufacturers have long shut down factories and outsourced everything to Asia for low-cost production. Executives are equally nonchalant when implementing SAP or CRM systems that demand re-engineering of innumerable workflows. Framed in this way, blockchain is actually less about new services or offerings that cannibalize existing businesses. Rather, it helps take costs out of a bulging baseline. Breakthrough innovation notwithstanding, blockchain is posed to support big banks in handling their voluminous transactions in years to come. And Wall Street knows this well.

So what will happen in the future after most banks have adopted blockchain? According to standard economic theory, a low-cost competitor enjoys cost advantage only when high-cost competitors still remain in the market. When everyone is using blockchain, the resultant saving will stop flowing in as corporate profit. Market competition will force all banks to pass on the hard-won saving back to consumers. Banking fees are set to plunge—which might as well be the greatest legacy of Satoshi Nakamoto.

NYT

# Envisioning Bitcoin’s Technology at the Heart of Global Finance

By [NATHANIEL POPPER](http://topics.nytimes.com/top/reference/timestopics/people/p/nathaniel_popper/index.html)AUG. 12, 2016



The World Economic Forum’s report is one of the strongest endorsements yet for the blockchain, the underlying technology introduced by the virtual currency Bitcoin. Credit Jean-Christophe Bott/European Pressphoto Agency

A new report from the [World Economic Forum](http://topics.nytimes.com/top/reference/timestopics/organizations/w/world_economic_forum/index.html?inline=nyt-org) predicts that the underlying technology introduced by the virtual currency Bitcoin will come to occupy a central place in the global financial system.

A [report](https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services) released Friday morning by the forum, a convening organization for the global elite, is one of the strongest endorsements yet for a new technology — the blockchain — that has become the talk of the financial industry, despite the [shadowy origins](http://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html) of Bitcoin.

“Rather than to stay at the margins of the finance industry blockchain will become the beating heart of it,” the head of financial services industries at the World Economic Forum, Giancarlo Bruno, said in a statement released with the report.

The blockchain originally referred to the database where all Bitcoin transactions are recorded and stored.

Unlike existing financial ledgers or databases used by banks and other institutions, the blockchain is updated and maintained not by a single company or government. Instead it is run by a network of users. It’s akin to the way Wikipedia is maintained by users around the globe.

## One Bitcoin Is Worth...

On Monday, one Bitcoin was worth [$567.](https://blockchain.info/charts/market-price)

The virtual currency — one that some people believe will transform the global financial system — has remained a mystery to many. [Here’s why](http://www.nytimes.com/2015/11/05/business/bitcoin-basics.html).

Source: Blockchain.info

Initially, bank executives shied away from endorsing Bitcoin because it had been used for drugs and crime. Now, however, many have focused on ways to create blockchains without using Bitcoins for transactions in any way.

This is attractive because blockchains — or “distributed ledgers,” as they are often described — could offer a new way to move money and track transactions across borders and other networks in a more secure, transparent and effective way than the current system.

Distributed ledgers are often viewed as most attractive to industries with businesses that lack a central institution they can trust to keep their records.

The World Economic Forum report notes that most developments are likely to happen behind the scenes. So consumers won’t see the changes to infrastructure, but the changes could lead to cheaper and faster financial services. The report says the technology could help improve both mainstream transactions, like global payments and stock trading, and lesser-known areas like trade finance and contingent convertible bonds.

The 130-page report from the forum is the product of a year of research and five gatherings of executives from several major institutions, including JPMorgan Chase, Visa, MasterCard and BlackRock.

The report estimates that 80 percent of banks around the world could start distributed ledger projects by next year. Large central banks are also studying how the blockchain will alter the way money moves around the globe.

## Listen: ‘Bitcoin Divided,’ From Planet Money

The writer, Nathaniel Popper, joined NPR’s Planet Money to explore how a behind-the-scenes fight over Bitcoin spilled out into the real world. You can also hear this episode on [iTunes](https://itunes.apple.com/us/podcast/708-bitcoin-divided/id290783428?i=1000371627998&mt=2).

Most banks [have already put together](http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html) blockchain working groups and released research reports hailing the potentially transformative effect of the technology.

But few real-world uses of the blockchain have come to fruition, other than [Bitcoin itself](http://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html). That has led to some questions about whether the blockchain is the proverbial solution looking for a problem, rather than an innovation that will be used widely.

Existing virtual currencies have continued to struggle with security problems. One of the largest Bitcoin exchanges, Bitfinex, recently lost more than $60 million worth of Bitcoin [in a hacking](http://www.nytimes.com/2016/08/04/business/dealbook/bitcoin-bitfinex-hacked.html) — the latest of several such incidents.

The World Economic Forum report suggests that it will take some time for such problems to be worked out. In addition to the technology issues, the report says that the industry will have to work with governments to create standard rules and laws to govern transactions.

The report does not make a single mention of Bitcoin. That mirrors the pronouncements from banks, which have often said that they can harness distributed ledgers without using existing virtual currencies. Rather, these ledgers would be run by groups of institutions that want to keep common records.

Just this week, 15 global banks, including Wells Fargo and UBS, said that they had completed a prototype of a distributed ledger that could track trade financing around the globe — providing a single record for a series of scattered, hard-to-track transactions.

# How China Took Center Stage in Bitcoin’s Civil War <http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html?action=click&contentCollection=DealBook&module=RelatedCoverage&region=EndOfArticle&pgtype=article>

[点击查看本文中文版](http://cn.nytimes.com/business/20160630/china-bitcoin-investiment1/" \o "点击查看本文中文版" \t "_blank) [Read in Chinese](http://cn.nytimes.com/business/20160630/china-bitcoin-investiment1/" \t "_blank)

By [NATHANIEL POPPER](http://topics.nytimes.com/top/reference/timestopics/people/p/nathaniel_popper/index.html)JUNE 29, 2016

[Slide Show](http://www.nytimes.com/slideshow/2016/07/03/business/dealbook/mining-for-bitcoin-in-china.html)

[[](http://www.nytimes.com/slideshow/2016/07/03/business/dealbook/mining-for-bitcoin-in-china.html)](http://www.nytimes.com/slideshow/2016/07/03/business/dealbook/mining-for-bitcoin-in-china.html)

##### [Slide Show|10 Photos](http://www.nytimes.com/slideshow/2016/07/03/business/dealbook/mining-for-bitcoin-in-china.html)

#### [Mining for Bitcoin in China](http://www.nytimes.com/slideshow/2016/07/03/business/dealbook/mining-for-bitcoin-in-china.html)

#### [Mining for Bitcoin in China](http://www.nytimes.com/slideshow/2016/07/03/business/dealbook/mining-for-bitcoin-in-china.html)

[CreditGilles Sabrie for The New York Times](http://www.nytimes.com/slideshow/2016/07/03/business/dealbook/mining-for-bitcoin-in-china.html)

A delegation of American executives flew to Beijing in April for a secret meeting just blocks from Tiananmen Square. They had come to court the new kingmakers in one of the strangest experiments in money the world has seen: the virtual currency known as [Bitcoin](http://www.nytimes.com/2015/11/05/business/bitcoin-basics.html).

Against long odds, and despite an abstruse structure, in which supercomputers “mine” the currency via mathematical formulas, Bitcoin has become a multibillion-dollar industry. It has attracted major investments from Silicon Valley and a significant following on Wall Street.

Yet Bitcoin, which is both a new kind of digital money and an unusual financial network, is having something of an identity crisis. Like so many technologies before it, the virtual currency is coming up against the inevitable push and pull between commercial growth and the purity of its original ambitions.

In its early conception, Bitcoin was to exist beyond the control of any single government or country. It would be based everywhere and nowhere.

Yet despite the talk of a borderless currency, a handful of Chinese companies have effectively assumed majority control of the Bitcoin network. They have done so through canny investments and vast farms of computer servers dispersed around the country. The American delegation flew to Beijing because that was where much of the Bitcoin power was concentrated.

## Listen: ‘Bitcoin Divided,’ From Planet Money

The writer, Nathaniel Popper, joined NPR’s Planet Money to explore how a behind-the-scenes fight over Bitcoin spilled out into the real world. You can also hear this episode on [iTunes](https://itunes.apple.com/us/podcast/708-bitcoin-divided/id290783428?i=1000371627998&mt=2).

At the time of the meeting, held at the Grand Hyatt hotel, over 70 percent of the transactions on the Bitcoin network were going through just four Chinese companies, known as Bitcoin mining pools — and most flowed through just two of those companies. That gives them what amounts to veto power over any changes to the Bitcoin software and technology.

China has become a market for Bitcoin unlike anything in the West, fueling huge investments in server farms as well as enormous speculative trading on Chinese Bitcoin exchanges. Chinese exchanges have accounted for 42 percent of all Bitcoin transactions this year, according to an analysis performed for The New York Times by [Chainalysis](https://www.chainalysis.com/). Just last week, the Chinese internet giant Baidu joined with three Chinese banks to invest in the American Bitcoin company [Circle](https://www.circle.com/en).

But China’s clout is raising worries about Bitcoin’s independence and decentralization, which was supposed to give the technology freedom from the sort of government crackdowns and interventions that are commonplace in the Chinese financial world.

“The concentration in a single jurisdiction does not bode well,” said Emin Gun Sirer, a professor at Cornell and a Bitcoin researcher. “We need to pay attention to these things if we want decentralization to be a meaningful thing.”

The power of Chinese companies has already come to play a major role in a civil war that has divided Bitcoin followers over the last year and led to [the departure of one of the top developers](http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html) of the virtual currency. The dispute has hinged on technical matters as well as on bigger questions of what Bitcoin should look like in 10 or 20 years.

[Continue reading the main story](http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html?action=click&contentCollection=DealBook&module=RelatedCoverage&region=EndOfArticle&pgtype=article#story-continues-2)

[[](http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html)](http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html)

## [A Bitcoin Believer’s Crisis of Faith JAN. 14, 2016](http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html)

[Continue reading the main story](http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html?action=click&contentCollection=DealBook&module=RelatedCoverage&region=EndOfArticle&pgtype=article#story-continues-3)

New data on Bitcoin’s use reveals that most of the transactions come from exchanges — most of all, exchanges in China — where people speculate on the value of the currency. People using Bitcoin to buy or sell products or services are a small proportion of all transactions. Chainalysis assembled the data for New York Times.

The movement of Bitcoins in 2016

ORIGIN

FLOWS

DESTINATION

2,622.8

2,850.9

China

China

1,462.5

THOUSANDS

OF BITCOINS

Exchanges where Bitcoin can be bought and sold for Chinese currency

United States

1,431.1

Exchanges where Bitcoin can be bought in dollars

518.5

1,312.1

United States

Other currency

exchanges

633.2

Other currency

exchanges

225.8

727.5

Mining\*

608.0

Euro-based

exchanges

71.3

502.4

Euro-based

exchanges

377.2

Mining\*

253.8

312.1

Mixing services\*

157.6

Mixing services\*

58.9

160.5

Scams/Ponzi schemes

143.4

Scams/Ponzi schemes

23.4

117.6

Dark markets\*

Dark markets\*

85.4

77.7

Wallets\*

55.8

Wallets\*

8.7

59.0

Payment processors

15.0

Gambling

7.7

Gambling

3.4

Payment processors

5.4

6,132.9

6,132.9

GRAND TOTAL

\***Mining:** Bitcoins flowing from companies that “mine” new Bitcoins by solving computational problems and offering computing power to the Bitcoin network. **Mixing services:** Services that mix Bitcoin transactions together to obscure the source or the transactions, like a money laundering service. **Dark markets:** Bitcoins flowing to black market services that sell illegal goods for Bitcoin, inspired by the Silk Road online drug market. **Wallets:** Bitcoins coming to and from online services that hold Bitcoin wallets for individuals.  
  
Chainalysis, which crunches virtual currency data for financial firms and law enforcement, obtained this data by analyzing all the transactions on the public ledger of Bitcoin transactions, known as the blockchain. Chainalysis has a proprietary method of tying specific transactions to particular businesses. Data are for 2016 through June 1.

Source: Chainalysis

By The New York Times

#### Network Bottleneck

The American companies whose executives journeyed to the Grand Hyatt — including venture-capital-funded start-ups like [Coinbase](https://www.coinbase.com/?locale=en) and Circle — are fighting to make Bitcoin bigger. They hope to expand the capacity of the Bitcoin network so that it can process more transactions and compete with the PayPals and Visas of the world.

The current size of the network goes back to the early days, when Bitcoin’s founder, Satoshi Nakamoto, limited the amount of data that could travel through the network, essentially capping it at about seven transactions a second. As Bitcoin has grown more popular, those limits have caused severe congestion and led to lengthy transaction delays.

The American delegation in China had a software proposal, known as [Bitcoin Classic](https://bitcoinclassic.com/), that would change all that.

The Chinese companies, though, had the ultimate decision-making power over any changes in the software, and they did not agree with the American delegation. The Chinese had thrown in their lot with another group of longtime programmers who wanted to keep Bitcoin smaller, in part to keep it more secure. The Americans hoped to persuade the Chinese to switch sides.

In a hotel conference room, the American team of about a half-dozen people cycled through its PowerPoint slides, in English and Chinese, arguing for expansion of the network, most notably pointing to the long delays that have been plaguing the system as a result of the congestion. The Chinese representatives listened and conferred among themselves. The group took a break for a lunch of lamb and dumplings at a nearby mall.

Photo



Racks of computers at a server farm mining Bitcoin and Ethereum. Credit Gilles Sabrie for The New York Times

“We kept coming back and saying, ‘For better or worse, you have this leadership in the industry, and everyone is looking to you to show some leadership,’” said Brian Armstrong, chief executive of Coinbase.

Ultimately, Mr. Armstrong said, “We were unable to convince them.”

Some Bitcoin advocates have complained that the Chinese companies have been motivated only by short-term profit, rather than the long-term success and ideals of the project. Bobby Lee, chief executive of the Bitcoin company BTCC, which is based in Shanghai, bristled at that — and at the notion that the Chinese companies represent any sort of united front. He attended the April meeting and pointed out that the Chinese companies had disagreed among themselves on how urgent it was to make changes to the Bitcoin software.

He said the American companies failed to understand the power dynamics in the room that day. “It was almost like imperialistic Westerners coming to China and telling us what to do,” Mr. Lee said in an interview last week. “There has been a history on this. The Chinese people have long memories.”

[Continue reading the main story](http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html?action=click&contentCollection=DealBook&module=RelatedCoverage&region=EndOfArticle&pgtype=article#story-continues-5)

#### A Mining Powerhouse

The [mysterious creator of Bitcoin](http://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html), Satoshi Nakamoto, released the software in early 2009. It was designed to provide both a digital coin and a new way to move and hold money, much as email had made it possible to send messages without using a postal service.

From the beginning, the system was designed to be decentralized — operated by all the people who joined their computers to the Bitcoin network and helped process the transactions, much as Wikipedia entries are written and maintained by volunteers around the world.

Photo



Jihan Wu, the founder of Bitmain, which is often described in China as the world’s most valuable Bitcoin company. Credit Sim Chi Yin for The New York Times

The appeal of a group-run network was that there would be no single point of failure and no company that could shut things down if the police intervened. This was censorship-free money, Bitcoin followers liked to say. Decision-making power for the network resided with the people who joined it, in proportion to the computing power they provided.

The allure of new riches provided the incentive to join: Every 10 minutes, new Bitcoins would be released and given to one of the computers helping maintain the system. In the lingo of Bitcoin, these computers were said to be mining for currency. They also served as accountants for the network.

For the first few years, aside from its use as a payment method on [the Silk Road](http://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html), an online drug market that has since been shut down, Bitcoin failed to gain much traction. It burst into the world’s consciousness in 2013 when the price of the digital money began to spike, in no small part because Chinese investors began trading Bitcoins in large numbers.

Mr. Lee said the Chinese took quickly to Bitcoin for several reasons. For one thing, the Chinese government had strictly limited other potential investment avenues, giving citizens a hunger for new assets. Also, Mr. Lee said, the Chinese loved the volatile price of Bitcoin, which gave the fledgling currency network the feeling of online gambling, a very popular activity in China.

There has been widespread speculation that Chinese people have used Bitcoin to get money out of the country and evade capital controls, but Mr. Lee and other experts said the evidence suggests this is not a significant phenomenon.

## China’s Bitcoin Dominance

Chinese companies mined about 70 percent of all new Bitcoins produced in the last month. Miners receive Bitcoins and have decision-making power over changes to the Bitcoin software, roughly in proportion to the amount of computing power they devote to the network.

“No Chinese person is pushing for Bitcoin because it’s libertarian or because it’s going to cause the downfall of governments,” said Mr. Lee, who moved to China after growing up in Africa and the United States and studying at Stanford. “This was an investment.”

The extent of the speculative activity in China in late 2013 pushed the price of a single Bitcoin above $1,000. That surge — [and the accompanying media spotlight](http://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/#58168a8e2295) — led China’s government to intervene in December 2013 and cut off the flow of money between Chinese banks and Bitcoin exchanges, popping what appeared to be a Bitcoin bubble.

The frenzy, though, awakened interest in another aspect of the currency: Bitcoin mining.

Peter Ng, a former investment manager, is one of the many people in China who moved from trading Bitcoins to amassing computing power to mine them. First, he mined for himself. More recently he has created data centers across China where other people can pay to set up their own mining computers. He now has 28 such centers, all of them filled with endless racks of servers, tangled cords and fans cooling the machines.

Mr. Ng, 36, said he had become an expert in finding cheap energy, often in places where a coal plant or [hydroelectric](http://topics.nytimes.com/top/reference/timestopics/subjects/h/hydroelectric_power/index.html?inline=nyt-classifier) dam was built to support some industrial project that never happened. The Bitcoin mining machines in his facilities use about 38 megawatts of electricity, he said, enough to power a small city.

The people who put their machines in Mr. Ng’s data centers generally join mining pools, which smooth the financial returns of smaller players. A popular one, BTCC Pool, is run by Mr. Lee’s company. This month it attracted about 13 percent of the total computational power on the Bitcoin network. The most powerful pool in China — or anywhere in the world — is known as F2Pool, and it had 27 percent of the network’s computational power last month.

Photo



Because the computations involved in mining Bitcoin are so intense, the most important factor in determining the profitability of a mining operation are the electricity costs. Credit Gilles Sabrie for The New York Times

#### The Politics of Pools

Big pool operators have become the kingmakers of the Bitcoin world: Running the pools confers the right to vote on changes to Bitcoin’s software, and the bigger the pool, the more voting power. If members of a pool disagree, they can switch to another pool. But most miners choose a pool based on its payout structure, not its Bitcoin politics.

It was his role overseeing BTCC Pool that got Mr. Lee invited to the meeting with the American delegation in Beijing. The head of operations at F2Pool, Wang Chun, was also there.

Perhaps the most important player in the Chinese Bitcoin world is Jihan Wu, 30, a former investment analyst who founded what is often described in China as the world’s most valuable Bitcoin company. That company, [Bitmain](https://www.bitmain.com/), began to build computers in 2013 using chips specially designed to do mining computations.

Bitmain, which has 250 employees, manufactures and sells Bitcoin mining computers. It also operates a pool that other miners can join, called Antpool, and keeps a significant number of mining machines for itself, which it maintains in Iceland and the United States, as well as in China. The machines that Bitmain retains for itself account for 10 percent of the computing power on the global Bitcoin network and are enough to produce new coins worth about $230,000 each day, at the exchange rate last week.

Mr. Wu and the other mining pool operators in China have often seemed somewhat surprised, and even unhappy, that their investments have given them decision-making power within the Bitcoin network. “Miners are the hardware guys. Why are you asking us about software?” is the line that Mr. Ng said he often hears from miners.

This attitude initially led most Chinese miners to align themselves with old-line Bitcoin coders, known as the core programmers, who have resisted changing the software. The miners wanted to take no risks with the money they were minting.

But lately, Mr. Wu has grown increasingly vocal in his belief that the network is going to have to expand, and soon, if it wants to keep its followers. He said in an email last week that if the core programmers did not increase the number of transactions going through the network by July, he would begin looking for alternatives to expand the network.

However the software debate goes, there are fears that China’s government could decide, at some point, to pressure miners in the country to use their influence to alter the rules of the Bitcoin network. The government’s intervention in 2013 suggests that Bitcoin is not too small to escape notice.

Mr. Wu dismissed that concern. He also said that as more Americans buy his Bitmain machines and take advantage of cheap power in places like Washington State, mining will naturally become more decentralized. Already, he said, 30 to 40 percent of new Bitmain machines are being shipped out of China.

For now, though, China remains dominant.

“The Chinese government normally expects its businesses to obtain a leading role in emerging industries,” he said. “China’s Bitcoin businesses have achieved that.”

# ComputerWorld

# Blockchain: It's not just for finance anymore

* [](http://www.computerworld.com/article/3068223/emerging-technology/blockchains-split-personality-digital-disruption-or-digital-distraction.html%23tk.drr_mlt)

[Blockchain’s split personality: Digital disruption or digital distraction?](http://www.computerworld.com/article/3068223/emerging-technology/blockchains-split-personality-digital-disruption-or-digital-distraction.html#tk.drr_mlt)

* on IDG **Answers**

[How does 5G compare to 4G and when will it be available?](http://www.idganswers.com/question/29142/how-does-5g-compare-to-4g-and-when-will-it-be-available" \l "src=ctw" \t "_blank)



Credit: Shutterstock

## Blockchain powers virtual cryptocurrencies like Bitcoin. But despite its reputation as a financial technology platform it may prove to be highly valuable outside of finance, and particularly in the emerging world of mission-critical Enterprise of Things.

Computerworld | Aug 25, 2016 12:20 PM PT Like this article? *thumbsup* +2 *thumbsdown*

RELATED TOPICS

You’ve probably heard about [Bitcoin](http://www.computerworld.com/article/3038065/e-commerce/the-case-for-bitcoin.html" \t "_blank), the virtual cryptocurrency that has often been associated with illegal activities and the “dark web.” Indeed, it’s been a favorite way for drug dealers, for various criminals, and for hackers who take over machines and then demand “[ransomware](http://www.computerworld.com/article/3056705/security/ransomware-authors-use-the-bitcoin-blockchain-to-deliver-encryption-keys.html)” to get paid.

Since Bitcoin transactions are secure and essentially untraceable, it makes life much easier for undercover transactions. Of course, there are many legitimate uses for Bitcoin as well, and many mainstream institutions have begun accepting it as payment.

Bitcoin and similar types of cryptocurrencies are based on a technology called [blockchain](http://www.computerworld.com/article/3054215/cloud-computing/5-things-you-should-know-about-the-blockchain.html) (although there are some competitors, Blockchain is currently leading the field in vendor support and R&D). Blockchain in its simplest form provides a mechanism so that each step in the process chain has the ability to add data to a protected ledger and to determine that the data has not been changed or altered in any way. This creates a fully audited trail of any and all activities for a specific data set related to an activity or process.

In this way, blockchain provides for an unalterable history of all transactions and verifiable database of activities for use by any applications needing access to the ledger. Clearly this is important in any high value transaction that must be prevented from being forged and/or hijacked. Which is why blockchain is so attractive as a financial vehicle.

Use of blockchain in financial systems continues to expand and will be an increasingly important technology going forward. But blockchain capability may actually be as or more important to enabling a growing number of high value IoT functions that must also be effectively protected.

In the important field of the [Enterprise of Things (EoT)](http://www.computerworld.com/article/3100382/internet-of-things/the-enterprise-of-things-its-the-back-end-that-counts.html), having proof of unaltered data is often mission critical and can make the difference in a life or death situation, in hazardous response requirements, or in many other high value interactions/operations.

For example, imagine health related data from some monitors that could control life or death situations, being sent to the cloud for processing. How do you know that data is legitimate and unaltered?

Or perhaps a company is shipping very expensive drugs that must be maintained at a particular environmental level to remain effective. How do you verify the monitoring data is valid when high-priced product sales are at stake?

Or you may be monitoring data from a power plant or other large public facility. How do you verify the data has not been altered to mask some form of tampering that could cause the plant to fail, or worse? Or data sent from an operating automobile or truck? Or airplane?

There are a large number of such potential uses for EoT generated data that are of extremely high value and any attempts at altering or “spoofing” such data could have potentially monumental consequences. Which is why data protection and verification is of such high importance to many critical EoT solutions (and often overlooked and/or neglected).

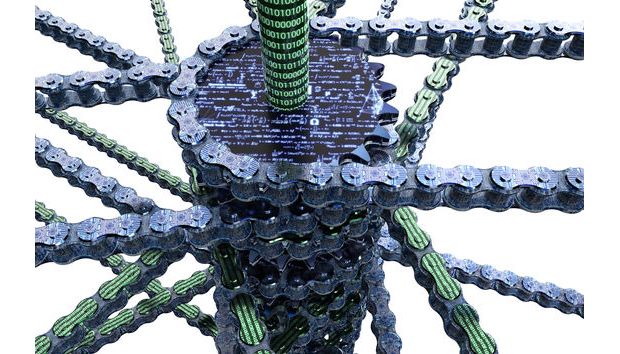
Many companies are investing in blockchain technology as part of their infrastructure capabilities. For example, [IBM](http://www.computerworld.com/article/3095395/cloud-computing/ibm-tests-secure-cloud-blockchain-service.html) as part of BlueMix has been promoting use of blockchain in its software targeted at financial institutions. But it may be equally as important to IBM in enabling Watson and its cognitive services for many industries required to fully verify all data before it is analyzed and acted upon.

And IBM is not alone. [Microsoft](http://www.computerworld.com/article/3051662/cloud-computing/microsoft-to-offer-blockchain-to-banks-with-new-partnership.html) Azure has made available a blockchain-as-a-service environment, as has Amazon (AWS). System integrators like PwC and Deloitte provide blockchain services. And the list is growing. In the next 1-2 years, I expect nearly all the major infrastructure vendors to offer services based on blockchain or a similar audited ledger technology.

So what does all this mean to the emerging field of EoT? As more and more organizations find ways to exploit the benefits of an EoT environment, they will be faced with a real security dilemma that requires a way to fully audit and verify that the data generated by the “things” and acted upon by analytics and automated workflow systems has not been compromised in any way. This is not only a nice to have, it’s potentially a requirement to prevent catastrophic circumstances.

While not the only way companies will have to deal with security in an EoT environment, blockchain and similar technologies offer an important step forward in making EoT safe from hacking and/or hijacking. I expect many vendors to start addressing such needs with targeted offerings. Companies serious about EoT need to fully examine the benefits of such a technology as a key component of their strategy going forward.

# IDG



# Hype vs. reality: We investigate the potential in blockchain

* 0
* Posted by [Kathryn Cave](http://www.idgconnect.com/author/212)
* on August 30 2016

At the end of last year Brave New Coin ran an [article titled](http://bravenewcoin.com/news/ten-companies-using-the-blockchain-for-non-financial-innovation/" \t "_blank): “Ten companies using the blockchain for non-financial innovation”. In the midst of all the hype about blockchain, this listicle probably provided the clearest view of how blockchain really can be used outside finance. This was because it offered practical examples that entrepreneurs are actually trying to make reality.

Some of the more interesting new companies in the space include better [digital rights for artists](https://www.ascribe.io/" \t "_blank), insight into the supply chain – for particular items, [like diamonds](http://www.everledger.io/" \t "_blank), and [across the spectrum](https://www.provenance.org/" \t "_blank) – along with a new service to “[backup your DNA](http://genecoin.me/" \t "_blank)”. I contacted a number of the companies listed but it is all such early days that nobody was prepared to be interviewed.

**What exactly is blockchain?**

As Ed Wallace, Director of Advanced Threats at [MWR InfoSecurity](https://www.mwrinfosecurity.com/" \t "_blank) explains: “Blockchain is just a record of transactions, like a double-entry book keeping system or ledger, that can be distributed – shared with whomever you want or is completely public – that uses encryption as a way of validating the entries are correct and can’t be changed.”

At an even more prosaic level it is a database. “What exactly could it do now that we couldn’t do with database technology like SQL before?” asked Luke Parker in the [Magnr Blog](https://magnr.com/blog/technology/private-vs-public-blockchains-bitcoin/" \t "_blank) recently. “Not much, really, and it would also be much slower than a SQL database. All of the advantages derived from basic blockchain technology can be boiled down to only two benefits; corruption resistance and redundancy.”

Rahul Singh, President of Financial Services at [HCL Technologies](http://www.hcltech.com" \t "_blank) spells out a pragmatic everyday use case which combines financial potential with other areas.

“Imagine a smart lock to a public toilet. Imagine now that it can be opened instantly by making a payment over a mobile app that is dictated by rules embedded in a smart contract using blockchain technology. When the rules are met, the lock opens. Money becomes the key, and the transaction is completed, securely and in an auditable manner.”

However, there is still a lot of debate and speculation about where the biggest opportunity really lies. Middlesex University recently produced an in-depth report titled “[Music on the blockchain](http://www.mdx.ac.uk/__data/assets/pdf_file/0026/230696/Music-On-The-Blockchain.pdf" \t "_blank)” [PDF]. While Mustafa Al-Bassam, IT security advisor at [Secure Trading](http://www.securetrading.com/" \t "_blank) believes “the biggest impact is likely to be in sharing economies and online marketplaces, by reducing middlemen fees”.

“For example,” he says “consider a flat rental marketplace on the blockchain, where there is no need for a company like Airbnb to take a cut – with a smart contract connected to a smart door that opens automatically upon payment without the need for physically transferring keys. This already exists today to some extent with [Open Bazaar](https://openbazaar.org/" \t "_blank), a decentralised online marketplace that uses Bitcoin and Slock.it, which is a start-up that lets you represent physical objects on the blockchain.”

Ron Hirson, head of product at [DocuSign](https://www.docusign.co.uk/" \t "_blank) adds further perspective “as with most technological breakthroughs, blockchain’s success depends almost entirely on its interpretation and application. To many the potential is huge. To others, it’s just a distributed database. It’s up to the first group to develop innovative use cases that convince businesses of its value.”

**How does blockchain fit in with Bitcoin?**

The public ledger for Bitcoin transactions is the most famous blockchain but it is by no means the only one. Yet the real split is between private and public blockchains.

Luke Parker presented an excellent discussion on the difference between private and public blockchains and [whether both can prevail](https://magnr.com/blog/technology/private-vs-public-blockchains-bitcoin/" \t "_blank) recently in the Magnr Blog. But the very short answer is that the main benefit of the public blockchain is that it is open and transparent – although this can, of course, throw up issues of its own – while private blockchains are much faster but have been described by popular Bitcoin speaker [Andreas Antonopoulos](https://antonopoulos.com/" \t "_blank) as akin to corporate intranets.

“If the [Bitcoin maximalists](https://www.chrisderose.com/video/what-is-bitcoin-maximalism" \t "_blank) are wrong about Bitcoin becoming a global monetary standard, it is likely that one of these top-level banking consortiums using a private blockchain will dominate the future of mainstream finance,” says Parker.

Luke Sully, Associate Partner, Blockchain Security Services Lead at [IBM](http://www.ibm.com/blockchain/" \t "_blank) tells us that there are hundreds of Proof of Concepts being developed for private blockchains by organisations all over the world at present.

“Essentially 2016 remains a Proof of Concept market,” he says “but key concepts and standards are still missing or only currently emerging to mature the technology. Many implementations aren't yet ready for serious business use yet.”

**Where are we now with blockchain?**

As Stephen Holmes at [VirtusaPolaris](http://www.virtusapolaris.com/" \t "_blank) FINtech Banking Lab points out “we are only at the beginning of the adoption curve for this disruptive technology”. The smart contracting platform, Etherium, for example, has been around for just one year – with the first block written on 30th July 2015.

Sinan Baskan, Solutions Director, Financial Services CTO Solutions at [MarkLogic Corporation](http://www.marklogic.com/" \t "_blank) believes even with the support of governments, global banks and corporations, this is a decade-long transformation.

In the government sphere the [UK clearly leads the way](http://www.idgconnect.com/blog-abstract/19200/uk-government-continues-blockchain-lead) although many other countries are taking interest. However, Ajay Vij, Vice President and Regional Head of Financial Services, Europe at [Infosys](https://www.infosys.com/" \t "_blank) believes in future “blockchain will be particularly useful in supporting government initiatives to protect citizen’s identities, tax collections and welfare payments from fraudulent misuse, while improving accuracy in state records.”

Yet government aside, Baskan feels “currently there’s not enough visible support for blockchain from more established companies such as IBM, who no doubt will be watching closely and making their own plans”.

“I doubt very much the key players will move quickly to rely on current solutions from start-ups and application vendors,” he adds “they will wait until the established players reveal their own plans.”

He also suggests that although cutting the time window on various transactions may be tipped as a benefit of blockchain in various financial organisations but “given other more pressing operational and competitive priorities and the huge up-front capital investment required, it is not clear who is complaining about the status quo and is ready to embrace blockchain”.

Like most potential changes this will not be good for everyone. Kerim Derhalli, CEO of [invstr](https://invstr.com/" \t "_blank) believes: “The implications for digital intermediaries such as custodians, stock exchanges and registries are potentially very negative – they will be the most vulnerable to dis-intermediation by blockchain-based technologies. These groups need to either embrace the technology now, or be disrupted by it.”

Singh of HCL Technologies agrees. “The evolution of the technology is relentless. Not only are use cases becoming interesting, but some developers are looking at parallel blockchains and sidechains that eliminate dependence on a single blockchain while improving scalability. This only goes to show that the innovation around this technology is already boiling over.”

Luke Sully, Associate Partner, Blockchain Security Services Lead, [IBM](http://www.ibm.com/blockchain/" \t "_blank) adds: “What's fascinated me, as someone who has looked at the growth of this technology since 2012, is how quickly the concept of blockchain has permeated public consciousness and how open organisations have been to thinking about their business in such a drastically different way. We continue to call blockchain technology ‘revolutionary’, we are building blockchains, investing in open source blockchain projects and working with hundreds of clients on this. It’s a strategic imperative for us globally.”

Victor Lynsenko, VP [Acronis Blockchain Solutions](http://www.acronis.com/en-us/business/blockchain-notary/" \t "_blank) seconds this adding that blockchain “keeps gaining momentum, investments in it keep growing and new use cases are uncovered, its applications and business benefits are quickly being exposed”.

In terms of more concrete timescale Stephen Holmes at [VirtusaPolaris](http://www.virtusapolaris.com/" \t "_blank) FINtech Banking Lab feels that initial deployment of blockchain solutions inside banks is likely to happen late 2016 to early 2017. “In the financial services community, a standards consortium is now in place (R3CEV); standards for exchange of blockchain information between participants are currently being drafted, and will likely come to fruition in the next two years.”

Adrian Shedden, head of fintech at law firm [Burges Salmon](https://www.burges-salmon.com/" \t "_blank) is more cautious though. He believes initial scaled commercial use will arrive by 2020 with wide-spread multi-sector use by 2025.

**What is the truth about the hype?**

Most of the people I’ve spoken to in the course of researching this piece believe that there is huge potential in blockchain which goes a lot further than hype.

Shedden of Burges Salmon clarifies, “with the likes of R3 CEV, Deloitte and the Bank of England, the FCA, Parliament and other heavy hitters getting involved we’re certainly beyond hype.”

Michael Cooper, BT’s CTO for [Radianz Services](http://www.globalservices.bt.com/uk/en/products/radianz" \t "_blank) says while this is not without hype he does believe the opportunity is significant. “There’s no shortage of postulating about blockchain potential. However, we do think the integration of blockchain technology with machine learning, artificial intelligence, behavioural analytics and similar technologies is potentially very interesting.”

This will allow users to obtain intelligence and insight from the data that is encoded in the blockchain, such as detection of behaviours, identification of fraud, developing provenance, he explains.

There are, of course, problems associated with all the hype though. As Andersen Cheng, CEO at [Post-Quantum](https://post-quantum.com/" \t "_blank) puts it blockchain “has been hyped up as being the solution to every problem in the world”.

“This includes everything from tracking parking tickets to valuable paintings,” he says. “To put this into context, this attitude is akin to saying Excel is a wonderful and useful tool to record entries, which is fine. However, it is not an end-to-end solution and does not address the fundamental audit points of such records' completeness, accuracy and validity at the point of entering a ledger which leads to a ‘rubbish in, rubbish out’ syndrome.”

Mustafa Al-Bassam, IT security advisor at [Secure Trading](http://www.securetrading.com/" \t "_blank) agrees. “I think the large companies and banks are talking about the wrong things when it comes to blockchain. They're talking about private blockchains, which are fundamentally no different than a fancy Excel spreadsheet, whereas the people at the heart of the movement are talking about completely different things. The large banks are trying to adopt blockchain technology in a way that they would like to see according to their business structure, but also in a way that doesn't make practical sense if you understand the technology.”

The difficulty with blockchain technology is that, because it's fundamentally structurally different than existing systems, there's a massive adoption barrier for people, he explains. This means it could be many years before it becomes the norm everywhere, if it does. If large businesses are smart about adopting it, I suspect we might see more B2B use cases of smart contracts first, before it gains mass consumer adoption.

“Unfortunately I do see a large number of proposals for blockchain use cases that should not be done on a blockchain at all but on standard web technology,” he concludes. “This could harm the industry in the short-term, but at the end of the day the actual realistic use cases will come to fruition.”

# WP

# The bizarre world of bitcoin ‘mining’ finds a new home in Tibet

By [Simon Denyer](http://www.washingtonpost.com/people/simon-denyer) September 12 at 4:02 PM

  
Set in remote mountains on the edge of the Tibetan Plateau, the bitcoin “mine” is strategically placed next to a hydroelectric power plant. (Paul Ratje/For The Washington Post)

Inside a metal shed in the Tibetan highlands of western China, thousands of microprocessors flank narrow corridors, generating a constant hum and stifling waves of heat.

Outside, the sky is clear and blue, with a mountain peak looming at the top of a narrow wooded valley. A flock of goats ambles idly past a pile of discarded foam packaging. Inside, though, tranquility is transformed into clamor. Red, blue and green lights constantly flash; cooling water trickles down the walls, and large ventilation fans thrum as they struggle to shift the hot air produced by all this concentrated computing power.

This is a bitcoin “mine,” the engine room of the world’s leading digital currency. The microprocessors here approve and record all the transactions that keep the bitcoin system running. They also compete to solve complex mathematical problems and are rewarded with bitcoins: That’s a way of putting fresh digital currency into circulation and incentivizing more people to set up “mining” operations.

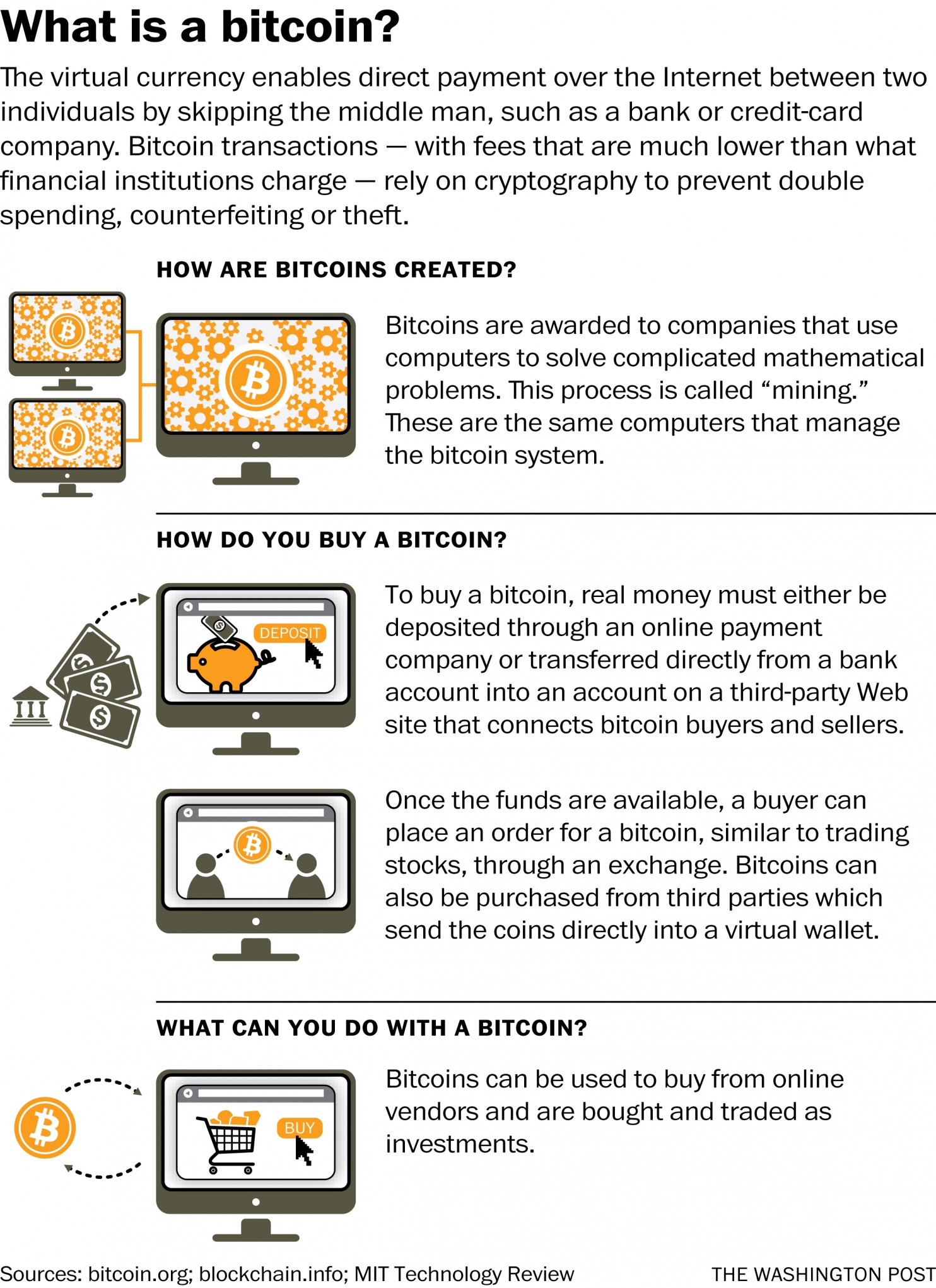
Bitcoin began as a utopian, libertarian dream, a decentralized currency outside the control of governments, a system that gives its users the anonymity of cash and the instant, global power of email. This was a system built not just for convenience but also for those who can’t bring themselves to trust the global financial system, created by a programmer whose identity remains a mystery.

Across Tibet, China is busy pulling mineral resources out of the ground; there is even a gold mine close by. But here in Kongyu, most of the mining is virtual. It is here because of extremely cheap hydropower, cheap wages — and perhaps because Chinese entrepreneurs have a knack for the business.

For a while, bitcoin was effectively kidnapped by drug dealers, becoming the anonymous payment backbone of the Silk Road, a black market in illegal drugs that flourished on the dark Net — until the FBI closed that market down in 2013.

Today it is an industry that is starting to come of age, but whose center of gravity has shifted to China, and away from utopian dreamers toward venture capitalists.

“When bitcoin was invented, the people dedicated to it were mostly crypto-punks and libertarians,” said [Eric Mu](http://www.coindesk.com/my-life-inside-a-remote-chinese-bitcoin-mine/), the chief marketing officer with HaoBTC, which operates the bitcoin “mine” in this township in China’s western Sichuan province. “Now they are more like bankers and lawyers who see opportunities in the industry. And as they join, the industry is changing.”



In this case, changing also means moving to China.

Today, mines run by Chinese companies account for about 70 percent of the world’s bitcoin processing power, its factories produce the cheapest microprocessors to run these mines, and its exchanges account for about 70 percent of the world’s bitcoin trade.

It is increasingly big business. Altogether there around more than 15 million bitcoin in existence: Each is worth $615 at current prices, with a market capitalization of $9.2 billion.

For some, Chinese domination of an industry once controlled by libertarian crypto-punks is a rich irony. [For others](https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7" \l ".nfsu4dwub" \t "_blank), it is more practical threat: Chinese miners, some argued, have been standing in the way of reforms needed to speed up transaction speeds on bitcoin’s fast-expanding network of users.

But those concerns might be overblown.

“Some people in the Western world were painting Chinese miners with too broad a brush,” said [Emin Gün Sirer](http://hackingdistributed.com/" \t "_blank), a computer science professor at Cornell University. “It’s not the case that all Chinese miners are part of the same enterprise or are colluding.”

  
Guo Hua, a site manager, checks equipment in a center in China’s Sichuan province, on Aug. 12. (Paul Ratje/For The Washington Post)

But Sirer identifies one risk with the concentration of mining power here: If the Chinese government wanted, it could in theory crack down on miners and force them to block certain bitcoin accounts.

“They would not be able to usurp funds, but they could stop the motion of funds,” he said, describing exactly the sort of government control bitcoin was supposed to guard against.

These are concerns that have parallels with the way China is using its digital market power to reshape the Internet and influence the global debate about censorship and surveillance.

But here, in the mountains of Sichuan, it is hard to see much evidence of a Chinese plot to bring bitcoin to heel.

The Chinese government has employed a fairly light touch. Although it banned banks from taking part in bitcoin trading in 2013, it left ordinary people free to buy and trade the crypto-currency, and miners free to operate.

The industry is run by a disparate mix of investors and dreamers, and manned by electricians and IT experts. There are people like Ryan Xu, an infectiously enthusiastic Chinese-born Australian who first became interested in libertarian economics while working as a reactor operator in a nuclear power plant. He now describes himself as “both a utopian and a venture capitalist.”

“We need to foresee the next five or 10 years,” he said in a wide-ranging conversation over dinner in the western city of Kangding. “All the governments are printing money and diluting people’s wealth. Is that justice or robbery? The financial system also keeps crashing every five or 10 years. I think that’s an illness in the monetary system and it needs a cure.”

He says he is not sure bitcoin is the answer, but it is at least an experiment that might work.

So why China?

Running microprocessors sucks electricity. Competition is intense and profit margins are narrow: Xu has moved his mines around the world in search of the cheapest power, from Iceland to Georgia, and then to Washington state, from the coal fields of China’s northern Inner Mongolia province and now to the mountains of Sichuan.

  
Thousands of microprocessors approve and record all the transactions that keep the bitcoin system running. (Paul Ratje/For The Washington Post)

His latest mine is still under construction, between a hydroelectric power plant and the concrete shell of a disused power transmission station, between Kongyu and the city of Kangding.

As China’s economy boomed, private companies set up hydroelectric plants in western Sichuan; then, as the economy slowed, they found themselves unable to sell to the national grid, elbowed out of the market by more politically powerful state-owned firms.

“It took a lot of money to build the plants, but it doesn’t cost that much to maintain them,” said HaoBTC’s Mu. “So it makes sense for them to sell the power to anyone willing to buy, even at a low rate.”

Maintenance staff are cheaper here than in the West. Mu says his company employs 10 people at three mines in the mountains, paying them around 6,000 yuan ($900) a month, a “decent salary” for this part of the world. HaoBTC runs one other mine in Sichuan and one farther west in Xinjiang, with more than 11,000 machines, earning more than 80 bitcoin a day — a daily income stream worth more than $745,000.

But it is not only Chinese entrepreneurs who have taken to bitcoin. Deprived of good investment opportunities at home, and burned by a volatile stock market, a growing number of Chinese people have begun speculating and investing in bitcoin.

Bobby Lee, a former Silicon Valley engineer who founded China’s first bitcoin exchange, BTCC, attributes it partly to a natural instinct to buy and sell.

“If you look at Las Vegas or Macau or casinos worldwide, how come most of the clientele are of Asian descent, or Chinese specifically?” he asked. “It has to do with some cultural instinct. Chinese people like to gamble.”

Yet as bitcoin matures, it is also experiencing some significant growing pains.

On Aug. 2, the Bitfinex exchange in Hong Kong was forced to admit that [hackers had stolen](http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP" \t "_blank) nearly 120,000 bitcoin worth $72 million from customers’ accounts. That news caused the bitcoin price to fall by more than 20 percent, and underlined the safety concerns that many ordinary people feel about owning digital money.

At the same time, the system is showing signs of overloading. Bitcoin’s current technology can only process around three digital transactions a second — minuscule compared with the roughly 24,000 transactions per second that Visa can manage.

Delays in processing transactions have grown, as have transaction fees, and the industry has become [deeply divided](http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html?_r=0" \t "_blank) about how to reform the system to solve the problem.

  
Ryan Xu shows his company’s equipment in part of his latest mine, still under construction. (Paul Ratje/For The Washington Post)

[Jeff Garzik](http://garzikrants.blogspot.com/" \t "_blank), a leading bitcoin developer based in Atlanta, argues that a technological fix is in the pipeline that will allow soon bitcoin to process tens of thousands of transactions a second.

“I think that with new technologies coming down the pipeline, it can scale up to everyone buying their coffee with bitcoin in the entire world,” he said. “It really can be the first really good substitute for physical in-your-hand cash.”

Like Sirer, he isn’t too worried about the current concentration of mining power in China, partly because the market is so dynamic and the dominant players change every year.

“It’s much easier to challenge the dominant players in this space because market entry is so easy,” he said. “If the Chinese miners suddenly power off their rigs, within 24 hours we’ll see the emergence of another competitor.”

Here in the mountains, miners while away their free time playing mah-jongg or poker, smoking cigarettes or surfing on their smartphones. Site manager Guo Hua used to run a small camera-repair shop and still likes fiddling around with machines. Marketing manager Mu, who spends only a few weeks of the year here, likes to translate books in his free time or run to the nearest town to buy cigarettes for his colleagues. Sometimes he hikes into the mountains, toward a remote Tibetan village or a looming peak, a welcome change of change of pace from Beijing and its polluted air.

And all the time, the microprocessors keep on running.

# Coin Desk

# Blockchain Startup Chronicled Launches Ethereum IoT Registry

[Alyssa Hertig](http://www.coindesk.com/author/alyssa-hertig/) ([@AlyssaHertig)](http://www.twitter.com/AlyssaHertig) | Published on August 24, 2016 at 12:55 BST

News



In an effort to build a standard for the emerging Internet of Things (IoT), Chronicled is open sourcing a tool for registering connected devices on the ethereum blockchain.

Described as a "cross between Wikipedia and Carfax" for consumer goods, the [platform](http://chronicled.org/) will register the identities of near-field communication (NFC) and bluetooth low energy (BLE) chips, components of IoT that today allow smartphones to “talk” with other devices.

ADVERTISEMENT

While the IoT has been hailed as an inevitability, technology experts ague that a fragmentation of standards have held back its adoption. Today, industry companies are each developing their own way for devices to communicate, but [Chronicled](http://www.coindesk.com/tag/chronicled/)'s founders want to use the ethereum blockchain to make private IoT database registries interoperable.

Chronicled CEO Ryan Orr told CoinDesk:

"What’s missing is interoperability for all those chips so that when a consumer is out in the world, they can interact with their world in a ubiquitous, seamless way. Right now it’s completely broken."

So far, Chronicled has deployed 10,000 NFC and BLE chips, most of which are embedded in [limited edition sneakers](http://www.coindesk.com/chronicled-sneakers-blockchain-big-market/) or other apparel, and each device is matched with a record of identity on the ethereum blockchain to reduce counterfeiting of luxury items.

Sneakers are the company’s first use case, but the team’s goal from day "zero", according to Orr, was to transition to other consumer goods and to expand to a public blockchain database.

To achieve this, Chronicled is also collaborating with existing IoT companies, including semiconductor company Silicon Labs and [Blue Bite](https://www.crunchbase.com/organization/blue-bite), a New York-based BLE firm.

## Securing devices

As with other startups in the industry, Orr said he sees blockchains as a way to enable a machine-to-machine economy by which devices can more easily, and safely, interact.

"Machines need to have identities so that machines can come to a decision on whether or not to trust the other machine or to understand where it’s from, which services it might be able to offer," Orr argued.

He offered the example whereby an [Amazon drone](http://www.businessinsider.com/amazon-secret-drone-testing-site-cambridge-discovered-2016-8) would deliver a package through the window of a home. Using IoT devices, he said, the window could verify instantly whether or not the drone is safe, potentially with public information off of the Amazon website, and enable the drone to drop off real-world goods.

"Verifying the identity of a device in a secure and public way is the first step to doing hundreds of different things on top of it," Orr said.

A key attribute that makes blockchains primed for such use cases, according to the team, is that anyone can use it to register a device.

This is something that third-party developers are more likely to want to build on, Orr asserted.

## Why ethereum

With the announcement, the company is releasing tools for developers, including starter kits, SDKs and an “Open Registry Explorer” so that any developer can use the platform to tag devices themselves. But a key component will also be [ethereum](http://www.coindesk.com/technology/smart-contracts-news/ethereum/), a public blockchain platform.

Despite recent [setbacks](http://www.coindesk.com/the-dao/), Orr said that there were multiple "dimensions" to Chronicled’s decision to use ethereum over other blockchains. In particular, he pointed to its flexibility and transparency, which he said helps with the company’s goal of building an interoperable standard.

"The ethereum project is at a critical mass globally. It could become a global standard in respect to product authentication," he said.

It’s also worth noting that ethereum founder Vitalik Buterin is on board with the idea. "Consumer IoT has always been one of the areas of blockchain adoption that I have been most bullish about," Buterin said in a statement.

Other companies are also experimenting with combining the two budding technologies. Filament, for example, [raised](http://www.coindesk.com/filament-nets-5-million-for-blockchain-based-internet-of-things-hardware/) $5 in Series A funding last year to enable connected devices to communicate.

Orr said that Chronicled eventually hopes to partner with other companies, such as 21 Inc, to continue its work toward this goal.

# NYT

# Central Banks Consider Bitcoin’s Technology, if Not Bitcoin

By [NATHANIEL POPPER](http://www.nytimes.com/by/nathaniel-popper)OCT. 11, 2016

Photo



Lael Brainard, the Federal Reserve governor the overseeing new technology, says the decentralized method of record-keeping introduced by Bitcoin has the potential to transform multiple aspects of the financial system. Credit Yuri Gripas/Reuters

Bitcoin was created by libertarian-minded programmers with a deep suspicion of central banks and the national currencies they issue.

Yet it is central banks that are doing some of the most ambitious work of late in trying to harness the technology introduced by Bitcoin.

The central bankers do not want their institutions to own or use Bitcoin itself. Instead, they hope they can use the decentralized method of record-keeping introduced by Bitcoin — known as the blockchain or distributed ledger — to complete and record transactions in the real economy more efficiently, quickly and transparently.

The most enthusiastic central banks — including the [Bank of England](http://topics.nytimes.com/top/reference/timestopics/organizations/b/bank_of_england/index.html?inline=nyt-org) and the People’s Bank of China — have discussed issuing their national currencies onto some sort of distributed ledger, a name that comes from the concept of several parties keeping records simultaneously.

## Related Coverage

[[](http://www.nytimes.com/2016/08/04/business/dealbook/bitcoin-bitfinex-hacked.html)](http://www.nytimes.com/2016/08/04/business/dealbook/bitcoin-bitfinex-hacked.html)

## [Bitcoin Plunges After Hacking of Exchange in Hong Kong AUG. 3, 2016](http://www.nytimes.com/2016/08/04/business/dealbook/bitcoin-bitfinex-hacked.html)

[[](http://www.nytimes.com/2016/05/28/business/dealbook/paper-points-up-flaws-in-venture-fund-based-on-virtual-money.html)](http://www.nytimes.com/2016/05/28/business/dealbook/paper-points-up-flaws-in-venture-fund-based-on-virtual-money.html)

## [Paper Points Up Flaws in Venture Fund Based on Virtual Money MAY 27, 2016](http://www.nytimes.com/2016/05/28/business/dealbook/paper-points-up-flaws-in-venture-fund-based-on-virtual-money.html)

[[](http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html)](http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html)

## [A Bitcoin Believer’s Crisis of Faith JAN. 14, 2016](http://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html)

[[](http://www.nytimes.com/2015/11/05/business/bitcoin-basics.html)](http://www.nytimes.com/2015/11/05/business/bitcoin-basics.html)

## [Bitcoin Basics NOV. 4, 2015](http://www.nytimes.com/2015/11/05/business/bitcoin-basics.html)

Blockchains allow several different players to keep a shared spreadsheet using cryptography and so-called consensus mechanisms that provide a way to agree on which transactions happened at what time.

For the central banks, the promise of the technology is that it would allow them to track every pound or renminbi on every step of its travels through the financial system in real time — something that is impossible now. The goal would be to make the financial system more transparent, fast, efficient and secure.

If the central banks succeed, it would be one of the greatest unexpected twists in new technology: An invention aimed at dethroning central banks and making it harder for money to be tracked instead ends up empowering those central banks and making money more easily traceable.

The Bank of England has produced several research papers on the topic. One suggests that the economic benefits of issuing a digital currency on a distributed ledger could [add as much as 3 percent](http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf) to a country’s economic output, thanks to the efficiency it could offer.

A deputy governor at the People’s Bank of China, Fan Yifei, [wrote for Bloomberg View](https://www.bloomberg.com/view/articles/2016-09-01/on-digital-currencies-central-banks-should-lead) that “the conditions are ripe for digital currencies, which can reduce operating costs, increase efficiency and enable a wide range of new applications.”

And in [a speech o](http://www.federalreserve.gov/newsevents/speech/brainard20161007a.htm)n [Friday](http://www.federalreserve.gov/newsevents/speech/brainard20161007a.htm), [the Fed](http://topics.nytimes.com/top/reference/timestopics/organizations/f/federal_reserve_system/index.html?inline=nyt-org) governor overseeing new technology, Lael Brainard, said the technology had the potential to transform multiple aspects of the financial system.

“We are paying close attention to distributed ledger technology, or blockchain, recognizing this may represent the most significant development in many years in payments, clearing and settlement,” Ms. Brainard said.

Even the central bank officials who are most enthusiastic about these experiments say it will be years before any central bank issues its own currency onto a live distributed ledger.

Some critics say the public interest in the blockchain has been all talk and no substance — an easy way for stuffy central bankers to appear hip and relevant.

David Andolfatto, a researcher at the Federal Reserve Bank of St. Louis, said many of the central banks looking at blockchain technology would be better served by spending time and energy in updating the current software that underlies the financial system.

“If you take a snapshot of the existing plumbing, it looks a bit ugly,” Mr. Andolfatto said. “There’s nothing magical about a blockchain in solving this problem.”

Even within the Fed, though, other researchers and officials have expressed more excitement about the technology.

A week before Ms. Brainard of the Fed gave her speech on distributed ledgers, the chairwoman of the Fed, Janet L. Yellen, was asked about the technology at a congressional hearing. She said that “innovation using these technologies could be extremely helpful and bring benefits to society.”

The Fed has been pushed to act by the big banks that it regulates, many of which are experimenting with distributed ledgers as a way to settle trades and record data and transactions. Just last week, JPMorgan Chase said it was moving toward a public release this year of its “enterprise grade” blockchain.

Most financial institutions and central banks are looking at distributed ledgers that would be maintained on the computers of all the major players in the financial system, including the central bank and the biggest financial institutions.

In the systems being discussed, each player in the system would communicate with all the others anytime money moved in the system, allowing everyone to update the ledgers on their computer systems simultaneously. This would provide multiple backups if the central bank’s computers came under attack. It would also hypothetically allow them to complete transactions much more quickly, and would make it easier to spot rogue actors.

Eric Piscini, who oversees work on blockchain by the consulting firm Deloitte, said that a year ago, central banks were looking at the technology mostly because they wanted to understand what private banks were talking about.

Now, he says, the central banks are embracing the technology to revamp their own infrastructures.

At the headquarters of the Netherlands’ central bank in Amsterdam, Ron Berndsen set up five laptops to run an experimental virtual currency, derived from the Bitcoin software. The coins issued in the system were nicknamed Dukatons, after a 17th-century silver coin used in the time when the Netherlands was a part of the Spanish Empire.

Mr. Berndsen operated the Dukaton system for three months to see what would happen if the central bank were setting the rules and did not have the same limits as Bitcoin. While the experiment was a success, he is now thinking much bigger and is in constant conversation with other central bank officials who are looking at ways to put their own currencies on distributed ledgers.

“There are so many things going on that it is hard to keep track of all the contacts,” said Mr. Berndsen, the head of market infrastructure at the Dutch central bank. “I hear from other central bank colleagues that it is the same everywhere.”

The experimentation so far has taken on many different forms and contemplated many different roles for distributed ledgers to play in the financial system.

Photo



Making a payment with Bitcoin Credit Arnd Wiegmann/Reuters

The Russian national bank [said last week](https://www.cbr.ru/Eng/press/?PrtId=event&id=643&PrintVersion=Y) that it had worked with a consortium of Russia’s biggest banks to develop its own distributed ledger, which it dubbed Masterchain. The Russian institutions have been sending messages on the system but are also looking at it as a potential “component of the new-generation financial infrastructure in the future.”

The Bank of Canada teamed up with the nation’s five largest banks — and the blockchain consulting firm R3 — for what was known as Project Jasper. In a simulation run this summer, the central bank issued so-called CAD-Coins onto a blockchain similar to the one that underlies the Bitcoin alternative known as Ethereum.

The banks used the CAD-Coins to exchange money — in this case fictional money — the way they do at the end of each day to settle their master accounts.

Carolyn Wilkins, senior deputy governor of the Bank of Canada, said in an interview that while the experiment was a success, a great deal of testing is still necessary before the bank can decide whether distributed ledger technology is ready for the real world.

Critics of blockchain technology have noted the apparent contradiction in central banks’ looking to distributed ledgers.

The blockchain was created to allow Bitcoin transactions to be recorded communally so that a central authority, such as a central bank, would not be necessary. If a central bank is involved and keeping track, why go to the trouble of keeping records communally?

The distributed ledgers being discussed by central bankers also generally lack the openness that has been one of the most attractive attributes of the Bitcoin network.

With Bitcoin, anyone can join the network and help support it, which has helped it win a following. The distributed ledgers being considered by the financial industry and central banks would generally allow only a small number of registered entities to join in and take part in the network.

Mark Carney, the head of the Bank of England, and perhaps the most prominent champion of distributed ledgers, [has said](http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf) that the technology could be worth using for central banks because it would make for a financial system that does not go down even if the central bank’s computer systems are temporarily taken offline.

The Bank of England [said last month](http://www.bankofengland.co.uk/markets/Documents/paymentsystem/cp160916.pdf) that it wanted the next version of the bank’s basic software infrastructure to be compatible with distributed ledgers.

Ms. Wilkins said the Bank of Canada was interested in the technology as a way to build a single, shared record of all the transactions among several institutions. That could leave much less money sitting idle while banks reconcile their different ledgers, as now happens.

It would also create a standardized way of recording transactions that would allow all the players in the system to communicate more seamlessly**.**

“There is currently a whole industry set up to reconcile and audit all these separate ledgers, and you can’t easily connect them,” she said. “This comprehensive shared data source could be a real benefit.”

# Forbes

Nov 1, 2016 @ 11:51 AM **1,517** views [The Little Black Book of Billionaire Secrets](http://bit.ly/29fF72b" \t "_self)

# How Blockchain Could Help To Make The Food We Eat Safer... Around The World

*      

By Bridget van Kralingen, IBM

The focus on safety throughout the global food supply chain is at an all-time high, but for all the wrong reasons. The numbers of people sickened by contaminated food products continues to escalate and recalls are issued with increasing frequency.

Like virtually every other complex issue in a world dominated by [data](http://www.ibm.com/big-data/us/en/big-data-and-analytics" \t "_blank) and how it’s used, the complex “system of systems” that is our global network of food production, inspection and distribution is primed for improvement via more open, transparent and fluid handling of information at every point in the journey from field to fork.

It’s high time. According to the [World Health Organization](http://www.who.int/mediacentre/factsheets/fs399/en/" \t "_blank), an estimated 600 million — or almost one in 10 people in the world — fall ill after eating contaminated food every year. And 420,000 of them die, which results in the subtraction of 33 million healthy life years from global societies and economies. The cost to individual lives is not the only substantial expense of foodborne illnesses.



In a recent [study](http://cfaes.osu.edu/news/articles/high-cost-foodborne-illness-new-study-provides-state-by-state-breakdown" \t "_blank) by Ohio State University, the estimated total national cost in the U.S. has spiked to $93.2 billion a year, or an increase of almost 20 percent in just the last four years. One looming issue is the food’s provenance because of the minimal amount of existing technology used to track food from the farm to plates

Recommended by IBM

To supply the world with millions of pounds of food, much of it must pass through many people, organizations, and governments that cultivate, influence or audit how it arrives to consumers. Collaboration and trust between governments, producers and suppliers is needed to re-establish consumers’ faith in the global food supply chain.

In a [recent survey](http://www.traceone.com/en/news/consumers-buy-private-brands-but-concerns-in-food-quality-and-safety-point-to-need-for-greater-transparency/" \t "_blank) by Trace One, 68 percent of consumers in the U.S. said they are not provided with enough information about what is in their food and its origins. More than 90 percent of consumers reported it is somewhat or very important to know where their food is coming from.

IBM is using blockchain to make the global food chain more transparent, authentic and trustworthy. Blockchain is like a computer’s operating system, regulating interactions. Because it creates an immutable digital record of these transactions, it is ideal for tracing the safety and authenticity of goods as they move from food suppliers to store shelves and consumers.

A recent IBM Institute for Business Value (IBV) [study](https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03771USEN&" \t "_blank) on blockchain in the supply chain found that by digitally tracking the provenance and movement of food throughout the entire supply chain, purveyors have instant quality assurance that the products they receive and serve customers are safe. With blockchain, this information flow can be widely shared to enhance decisions at all levels of the supply chain.

For example, “ready to eat” foods — such as frozen lasagna — top the list for recalled food products by a wide margin because they involve a large supply chain with multiple parties. Ready-to-eat food, once processed, typically requires a third party such as a logistics provider to transport the food to distribution warehouses.

Sometimes another supply chain partner provides this service and then often another intermediary provider will deliver the food from the warehouse to the store. That’s not only expensive, but maintaining the quality standards set by regulators by the U.S. Department of Agriculture to keep perishable products safe is also a challenge, particularly when the product contains frozen meat, vegetables or milk products.

Putting this transaction record on the blockchain can create significant savings in time, cost and transparency. Blockchain can transparently track the provenance of goods as they are passed from one organization to the next, building awareness and trust.

Scientists from IBM Research and researchers from Tsinghua University are working alongside top talent in transaction security and authentication technology from Tsinghua University and with Walmart’s expertise in supply chain, logistics and food safety, [to create a new model](http://www-03.ibm.com/press/us/en/pressrelease/50816.wss" \t "_blank) for food traceability, supply chain transparency and auditability using IBM Blockchain based on the open source Linux Foundation Hyperledger Project fabric.

The collaboration of Walmart, IBM and Tsinghua University takes advantage of the distinctive strengths of each member of the team. Scientists from IBM Research – China are among the leading-edge technologists at IBM now in the forefront of the rapid evolution of blockchain. This can help retailers like Walmart better supervise and manage the shelf life of products and reduce the risk of non-compliance in individual stores, ensuring that consumers are getting authenticated, safe products. Which is exactly the answer required.

**Tweet this:** [How to keep food safer using #blockchain technology by @IBM SVP Bridget van Kralingen @Forbes](https://twitter.com/intent/tweet?url=http%3A%2F%2Fwww.forbes.com%2Fsites%2Fibm%2F2016%2F11%2F01%2Fhow-blockchain-could-help-to-make-the-food-we-eat-safer-around-the-world%2F&text=How%20to%20keep%20food%20safer%20using%20%23blockchain%20technology%20by%20%40IBM%20SVP%20Bridget%20van%20Kralingen%20%40Forbes" \t "_blank)

Bridget van Kralingen is Senior Vice President of Global Industry Platforms at IBM.

# Knowledge @ Wharton

# Is Blockchain the Next Great Hope — or Hype?

Jan 11, 2017

* [North America](http://knowledge.wharton.upenn.edu/region/north-america/)



Cryptocurrencies such as bitcoin may have captured the public’s fancy – and also engendered a healthy dose of skepticism — but it is their underlying technology that is proving to be of practical benefit to organizations: the blockchain. Many industries are exploring its benefits and testing its limitations, with financial services leading the way as firms eye potential windfalls in the blockchain’s ability to improve efficiency in such things as the trading and settlement of securities. The real estate industry also sees potential in the blockchain to make homes — even portions of homes — and other illiquid assets trade and transfer more easily. The blockchain is seen as disrupting global supply chains as well, by boosting transaction speed across borders and improving transparency.

These uses are merely the tip of the proverbial iceberg for a nascent technology whose development stage has been compared to the early years of the internet. “We’re very early in the game,” said Brad Bailey, research director of capital markets at Celent, at a recent Blockchain Opportunity Summit in New York. He likened the blockchain’s current status to the web of the early 1990s, heralding a coming wave of new ideas and uses. “This will impact the world.”

The blockchain technology came about initially as a way to verify bitcoin transactions online and to enable two parties to transact business without having to know or trust each other. It was designed without a central authority in mind, such as a bank or government, to oversee transactions. Essentially, the blockchain is a shared virtual public ledger where encrypted transactions are confirmed by outside parties. In the bitcoin world, these outside parties are called “miners” — computers that solve complex mathematical problems to confirm transactions and earn fees. Confirmed transactions are placed in a “block” and added to the chain. Since the ledger is shared by everyone on the network, it is thought to be nearly impossible to remove or change the data – a premise that turned out to be false in some cases.

Today, the concept of the blockchain has expanded beyond its use by cryptocurrencies. Instead, the benefits of the shared ledger and its seemingly immutable record of transactions accessible to multiple parties are being explored by a variety of industries. Experts said there won’t be a “mother blockchain,” but multiple ledgers with different purposes. Varying versions of blockchains have popped up, too: While the original bitcoin blockchain was open to anyone, some companies’ blockchains are private and “permissioned” — they restrict access to approved parties. The latter approach is preferred by companies fearful of being hit with government fines and lawsuits if they get hacked, said summit participant Sarab Sokhey, chief technology leader of new product innovations at Verizon Wireless. They’ll stay private until the technology matures and industry standards are set.

“[The blockchain] could provide an identity to those who don’t have it, or promote financial inclusion.” –[Saikat Chaudhuri](http://knowledge.wharton.upenn.edu/faculty/saikatc/)

While the blockchain’s business applications are clear, it has social implications as well. For instance, it can create identities for individuals apart from those sanctioned by governments and not limited by geographic boundaries. The blockchain also allows less-technologically advanced nations to participate in global transactions more easily. “Blockchains are exciting, undoubtedly,” said Saikat Chaudhuri, executive director of the [Mack Institute for Innovation Management](https://mackinstitute.wharton.upenn.edu/" \t "_blank), which was an official partner for the summit. “It’s much more than about transaction efficiency or flexibility. It’s really beyond that. It could provide an identity to those who don’t have it, or promote financial inclusion. Therein lies the power of this whole thing.”

**‘Nervous’ Financial Institutions**

According to a survey by the IBM Institute for Business Value and the Economist Intelligence Unit, one in seven companies it calls “trailblazers” expect to have blockchains in production and at commercial scale in 2017. Respondents were interested in taking advantage of the blockchain’s multiple benefits, which include cost reduction, immutability of records, transparency of transactions and the potential to create new business models. For example, the blockchain would eliminate the need for keeping multiple records at banks and other parties doing currency trades. The survey tracked responses of 200 global financial markets institutions.

The survey also said “trailblazers” were focusing their efforts on the following business areas: clearing and settlements, wholesale payments, equity and debt issuance and reference data. The report added that in recent years, financial institutions have “swarmed to blockchain pilots and proofs of concept” — opening innovation labs, holding hackathons, partnering with financial technology startups, joining consortia and collaborating with regulators.

#### Sponsored Content:

To be sure, banks have a vested interest in participating. “Banks provide essentially escrow services for the transfer of value, and here comes a technology that threatens to eliminate that service,” said Chris Ballinger, global chief officer of strategic innovation at Toyota Financial Services. “So they are nervous about that, because it’s a huge revenue stream” that could be taken away. How? “With the blockchain, you can run a network that transfers value among untrusted nodes, and therefore you can eliminate the middle man and you can eliminate all the costs associated with the middle man,” he said. “You’re essentially turning assets into something like cash that you can hand to somebody and they will accept. That makes the transfer of assets extremely efficient.”

Another unique benefit of the blockchain is that it separates someone’s identity from the transaction they’re making. In general, a blockchain uses a digital signature – not real names and other personal information – that is activated by a private key or secret code held by the one doing the transaction. Compare that to current credit card or bank transactions, which tie one’s personal information such as a name and address to purchases and other financial activities. This separation improves the security of one’s data. “Today, the payments information and identity are [bound] together. The combined is a tempting honey pot for hackers,” Ballinger said. “By separating the financial information from the identity, there’s no honey pot, no central place to hack, no incentive to go after.”

In December 2015, Nasdaq [executed its first trade](http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326" \t "_blank) on a blockchain, through its Linq ledger. The exchange said the blockchain promises to expedite trade clearing and settlement – all the steps needed to transfer the asset from seller to buyer including recording the transaction — from three days to as little as 10 minutes. That’s because the trades remove many manual processes and bypass third parties. As such, “settlement risk exposure can be reduced by over 99%, dramatically lowering capital costs and systemic risk,” according to Nasdaq. Other stock exchanges tinkering with the blockchain include ones in Australia, Myanmar, Germany, Japan, Korea, London and Toronto.

Overstock.com is on the cusp of issuing its first security using the blockchain. “We are in the process of proving out the first public trading of a blockchain security,” said Ralph Daiuto, Jr., general counsel of tØ, a subsidiary of the e-commerce retailer. While the company has kept its clearing firm, it is using digital wallets for the actual transfer of assets in settlement of the trade. “The goal is to shorten the settlement cycle and [avoid] all the ills that can go wrong with that cycle.” He added that the company can cut its equity trading costs by 70% using the blockchain.

Overstock got regulatory approval for its blockchain trade by taking “incremental steps in proving out the technology in use cases and demonstrating we have real-world application for this blockchain technology,” Daiuto said. “It literally has been a monthly, if not a weekly, education process with our core regulators.” It has taken nearly two years of laying the groundwork for Overstock to get to this point.

**Real Estate and Smart Contracts**

An area of particular promise for the blockchain is the real estate market. “The blockchain solves pretty much every problem in real estate that we have” in terms of fraud, middleman fees and friction, opaque due diligence, slow price discovery, complex transaction process and other ills, said Ragnar Lifthrasir, president of the International Blockchain Real Estate Association. “In many ways, our technology is still in the 17th century – notaries still use seals.” The blockchain promises to simplify and speed up the process while adding transparency to the records.

“The blockchain solves pretty much every problem in real estate.” –Ragnar Lifthrasir

For example, in selling a house, people still sign paper deeds over to the new owner. It has to be entered into the public record, which means someone physically has to go to the local government office. “It’s a paper-based system that is ripe for fraud,” Lifthrasir said. The blockchain solution is fairly straightforward, using digital deeds. “When I want to transfer the property, I simply transfer it from my wallet to the buyer’s wallet.”

As for putting the property ownership on the public record, he said the list is already on the blockchain so recording it won’t be hard. Lifthrasir added that validation of ownership would be strengthened. “It’s very difficult to deny who owns the property when it’s on a public network.” His startup, Velox, is working with Cook County in Chicago to use the blockchain for transferring and recording property titles. It is also working on a way to show liens on titles on the blockchain.

Within a blockchain, so-called “smart” contracts could be revolutionary. “They programmatically represent a contract,” said Mark Smith, CEO of Symbiont and co-chair of the Smart Contract Council. For example, a smart contract on an auto loan could be linked in real time to payments made by the car buyer. If he misses payments, the contract gets wind of the violation and starts the repossession process. In Delaware, Smith’s company is working with the state to create “smart” records of its public archives to do such things as being able to sunset themselves.

EY’s Australian operations piloted a real estate blockchain ecosystem that is now being used in the market to trade full, and even fractional, ownership of properties. Real estate and financial institutions approved by EY all liked the idea of using a blockchain, but when it came to actual implementation, “fear and uncertainty crept in,” said James Roberts, partner and Australian blockchain leader. EY had to essentially guarantee verification of participants and transactions to build trust. “We decided we would solve the identity problem [of people and institutions]. We would build trust into the system and prove recordkeeping is true and accurate and can be used to transact financial instruments like property or debt.”

EY’s blockchain ecosystem goes through several stages. First, individuals using the blockchain have to be validated using identity checks and even biometrics. They create records on the blockchain using randomly generated unique keys that let EY do further checking against various databases from the government and elsewhere. Next, the transaction is traded on a blockchain exchange. The assets being traded are verified. The entire ecosystem is private and permissioned. Also, EY stores individuals’ unique keys offline for security. Moreover, EY built back-system administrative functions – despite the premise of the blockchain as not having a central authority – to make participants more comfortable in using the system. But to be a viable ecosystem, it needs to scale. “We need millions and millions of people in our system, and that’s going to take a lot of effort,” Roberts said.

“Once you give someone access to a network … they can end up very easily getting blanket access to that network.” –Joe Ventura

**Challenges and Risks**

Security is still the biggest challenge confronting the blockchain. “The truth is, once you give someone access to a network, many times, more often than not, they can end up very easily getting blanket access to that network,” said Joe Ventura, CEO of AlphaPoint. “This is a huge security problem.” However, if one ends up building many protections to prevent hacks, then it bogs down the blockchain and defeats its purpose in the first place. “Basically, you have to jump through so many hoops simply to pass the message from some party to another party.”

And while blockchain records theoretically can’t be changed, there are ways around that. Smith cited a recent controversial decision by the Ethereum Foundation – the organization behind the open-source cryptocurrency Ethereum – after a hacker exploited a software flaw and took funds. The foundation decided to roll back the clock to give people their money back and created two versions of the ledger. “Imagine if you’re a business and they roll back a day,” Ventura said. “That’s completely unacceptable.” Moreover, by creating two versions, some people were able to exploit it. “People were able to double their money,” Smith said.

As for compliance, at least regulators could have a node on the blockchain itself in which companies define their access to data, said Sandeep Kumar, managing director of Synechron. As such, regulators wouldn’t have to wait days for a bank to hand over documents for compliance. “They can see it as it is happening.”

In the end, each company has to figure out whether a blockchain is suitable. “Is it a blockchain use case or is it a database use case?” said Tyler Mulvihill, director of Consensys. “If you are a company that has a lot of information internally and you don’t transact like a lot of vendors, and not a lot of people need to use your information or do business with you, a database can be fine for a lot of things. It’s when you have a lot of parties that need trust, need access to certain information and need to be audited – that’s where I see the biggest use cases.”

# Computerworld

[News Analysis](http://www.computerworld.com/newsanalysis)

# FAQ: What is blockchain and how can it help business?

## The distributed ledger technology has enormous potential for firms that figure out how best to use it

[](http://www.computerworld.com/author/Lucas-Mearian/)By [Lucas Mearian](http://www.computerworld.com/author/Lucas-Mearian/)

Senior Reporter, Computerworld | Apr 24, 2017 3:01 AM PT

Credit: Thinkstock

Blockchain sounds like a way to keep boats anchored, which isn't a bad analogy, considering what the technology purports to do.

While some IT experts herald it as a groundbreaking way of creating a distributed, unchangeable record of transactions, others question the nascent technology's usefulness in the enterprise, which has traditionally relied on centrally administered databases to secure digital records.

Even so, companies are moving fast to try and figure out how they can use it to save time and money. And IT vendors are responding to customers calls for information, with some [already looking to include it as part of their services](http://www.computerworld.com/article/3190698/data-storage/for-enterprises-blockchain-isn-t-necessarily-a-good-fit.html).

**What is blockchain?** First and foremost, Blockchain is a public electronic ledger -- similar to a relational database -- that can be openly shared among disparate users and that creates an unchangeable record of their transactions, each one time-stamped and linked to the previous one.

Each digital record or transaction in the thread is called a block (hence the name), and it allows either an open or controlled set of users to participate in the electronic ledger. Each block is linked to a specific participant.

Blockchain can only be updated by consensus between participants in the system, and when new data is entered, it can never be erased. The blockchain contains a true and verifiable record of each and every transaction ever made in the system.

**Why is blockchain suddenly getting so much buzz?** In a word, [Bitcoin](http://www.computerworld.com/article/3038065/e-commerce/the-case-for-bitcoin.html" \t "_blank). Bitcoin is a wildly hyped cryptocurrency, a method of transacting payments over an open network using digital bits and encryption. It was the first ever decentralized one when it was created in 2009.

The term bitcoin was first... well, coined in 2008 when Satoshi Nakamoto [wrote a paper](https://bitcoin.org/bitcoin.pdf" \t "_blank) about a "peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."

**OK, so what exactly does blockchain do?** As a peer-to-peer network, combined with a distributed time-stamping server, blockchain databases can be managed autonomously. There's no need for an administrator. In effect, the users are the administrator.

**What industries are using it?** According to Angus Champion de Crespigny, Ernst & Young's Blockchain Leader, the technology is seen has being well suited to propagate security policies and identity access management.

The fact that each blockchain record contains a unique cryptographic hash that is used to track that block, as well as others in the associated chain, means the data cannot be modified, making it perfect for record keeping and auditing purposes.

[Financial services (see Bitcoin) has been the first industry to jump on board](http://www.computerworld.com/article/3124552/enterprise-applications/financial-sector-expands-use-of-blockchain-databases.html) the blockchain wagon. But other industries -- [such as healthcare](http://www.computerworld.com/article/3137490/enterprise-applications/article.html) -- have been quick to explore its use, too.

For example, IBM Watson Health and the U.S. Food and Drug Administration [are exploring the use of blockchain](http://www.computerworld.com/article/3156504/healthcare-it/ibm-watson-fda-to-explore-blockchain-for-secure-patient-data-exchange.html" \t "_blank) for secure patient data exchange, including sensitive electronic medical records, clinical trials and data culled from mobile devices and wearables.

While it's still early days, de Crespigny noted that more vendors are producing business-specific products, "which is really what's needed."

**How can it help those industries?** Blockchain eliminates huge amounts of recordkeeping, which can get very confusing when there are multiple parties involved in a transaction, according to Saurabh Gupta, vice president of strategy at IT services company Genpact. "Blockchain and distributed ledgers may eventually be the method for integrating the entire commercial world's record keeping," Gupta said in an email to *Computerworld*.

Genpact, for example, [just released a service](http://www.genpact.com/about-us/media/press-releases/2017-genpact-harnesses-blockchain-technology-to-transform-f-a-operations" \t "_blank) for finance and accounting that leverages blockchain-based smart contracts to capture all terms and conditions between a customer and an organization for an order.

Accenture recently released a report that claimed blockchain technology could reduce infrastructure costs for eight of the world's 10 largest investment banks by an average of 30%, "translating to $8 billion to $12 billion in annual cost savings for those banks."

The Bank of England [is considering ways](http://www.computerworlduk.com/data/bank-of-england-pushes-forward-with-blockchain-technology-for-settlements-3657464/" \t "_blank) that it can use blockchain for payments, clearing and settlement.

In another example, Acronis introduced blockchain technology in its [True Image 2017](http://www.acronis.com/en-us/personal/whats-new/?utm_medium=affiliates&utm_source=6161470&utm_campaign=cj&utm_content=10570888&utm_term=j1pbn2sv700113ap00624" \t "_blank) data backup software. The blockchain platform is used as a data certification and verification element -- a type of electronic document signing or notary service.

**Are there drawbacks to using it?** The same thing that makes blockchain attractive, its distributed nature, also makes it a potential security threat. In the enterprise, centralized control can translate into security. With blockchain, which is decentralized,  the technology works best when information sharing is a necessity across multiple, often disparate, parties.

Central control, as in a single administrator, can also be a double-edged sword since a single point of control is also a single point of failure, according to Serguei Beloussov, CEO of Acronis. While Beloussov himself believes blockchain is secure, he has several computer scientists on his staff that believe it's not -- and say it can be penetrated.

Then there's Satoshi Nakamoto. That could be one person's name or a pseudonym for a group of developers -- no one appears to know for sure. But Nakamoto holds 1 million bitcoins, or the equivalent to $1.1 billion. That has led some in Beloussov's company to speculate that the whole thing could be a giant Ponzi scheme, though there's no evidence to indicate that.

**Has the encryption ever been broken?** No. "That's not how this sort of thing will get broken. It'll get broken because of some insecurity in the software," said Bruce Schneier, a cryptographer and security expert. Schneier was referring to the fact that there are many versions of blockchain, such as [Ethereum](https://www.ethereum.org/" \t "_blank), a custom-built platform that was introduced in 2013 by then 19-year-old developer Vitalik Buterin. Additionally, vendors such as [Microsoft](https://azure.microsoft.com/en-us/solutions/blockchain/) and [IBM](http://www-03.ibm.com/press/us/en/pressrelease/51840.wss) have introduced blockchain capabilities in their software and services.

Alex Tapscott, the CEO and founder of Northwest Passage Ventures, a venture capital firm that invests in blockchain technology companies, said while no system is "unhackable," blockchain's simple topology is the most secure today.

"In order to move anything of value over any kind of blockchain, the network [of nodes] must first agree that that transaction is valid, which means no single entity can go in and say one way or the other whether or not a transaction happened. To hack it you wouldn’t just have to hack one system like in a bank… you’d have to hack every single computer on that network, which is fighting against you doing that."

The computing resources of most blockchains are tremendous, Tapscott pointed out [in an online interview](https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/from-big-data-to-smart-data-interview-alex-tapscott-blockchain.html), because it’s not just one computer but many computers. For example, the Bitcoin blockchain harnesses anywhere between 10 and 100 times as much computing power compared with all of Google’s serving farms put together.

"So again, not unhackable, but significantly better than anything we’ve come up with today," Tapscott said.

**Are there different blockchain permutations?** Yes. There are several general uses for blockchain platforms. There are public blockchains, which allow anyone to see or send transactions as long as they're part of the consensus process There are consortium blockchains, where only a pre-selected number of nodes are authorized to use the ledger. For example, a group of banks and their clearinghouse might use blockchain as part of the trade-clearing where each node is associated with a step in the verification process.

And there are private blockchains, where the ability to write to a ledger is restricted to a single organization.

**Where does it go from here?** Regardless of who developed it, businesses should always take a pragmatic approach when adopting any new technology, according to Gupta.

"You can't ignore it, but you can't just blindly adopt a new technology. The key is to see if it makes sense for your business problem," Gupta said.

Blockchain is emerging from concept to reality as products that use it are just now coming to market.

There are, however, more than 15 blockchain distributed ledger platforms being developed in parallel, with specialist applications on top of them, according to Gupta. The industry will need some standardization to encourage widespread adoption.

"Such challenges are common with new technologies," he said, "and even with this concern, blockchain is seeing a lot of interest.

# ComputerWorld

# Linux Foundation to develop tool for building blockchain business networks

## The open-source project would enable smart contracts to be developed for any number of industries

[](http://www.computerworld.com/author/Lucas-Mearian/)By [Lucas Mearian](http://www.computerworld.com/author/Lucas-Mearian/)

Senior Reporter, Computerworld | May 8, 2017 12:38 PM PT

* [](http://www.computerworld.com/video/48943/5-easy-data-visualizations-in-r%23tk.drr_mlt)

Video

[5 Easy Data Visualizations in R](http://www.computerworld.com/video/48943/5-easy-data-visualizations-in-r#tk.drr_mlt)

The Linux Foundation announced a new software project under its Hyperledger open consortium aimed at creating a collaboration tool for building blockchain business networks -- or smart contracts -- and their deployment across a distributed ledger.

The new project, called [Hyperleder Composer](https://www.hyperledger.org/blog/2017/05/03/meet-hyperledger-composer" \t "_blank), is a modeling language based on JavaScript and with REST API support, that allows non-developers and developers to model their business network. The language also supports modeling of relationships and data validation rules.

For example, all blockchain business networks share certain elements, such as assets, participants, identities, transactions, and registries. With existing blockchain or distributed ledger technologies, it can be difficult for organizations to take a blockchain business use case and map the concepts into running code.

Similar to public relational databases, [blockchain is a public electronic ledger](http://www.computerworld.com/article/3191077/security/faq-what-is-blockchain-and-how-can-it-help-business.html" \t "_blank) that can be openly shared among disparate users and that creates an unchangeable record of their transactions, each one time-stamped and linked to the previous one.

Blockchain ledgers can only be updated by consensus between participants in the system, and when new data is entered, it can never be erased. The blockchain contains a true and verifiable record of each and every transaction ever made in the system.

One of the most popular uses of blockchain is for "smart contracts," which allow electronic transactions to self-execute based on preset terms and conditions.

[Hyperledger](https://www.hyperledger.org/" \t "_blank), is a global, open source collaborative effort hosted by the Linux Foundation to advance cross-industry blockchain technologies.

All work done on Composer to date has been done on top of Hyperledger Fabric, a platform for developing applications atop the blockchain distributed ledger.

Composer, however, has been designed so that it can be ported to run on other distributed ledger technologies, such as [Hyperledger Iroha](https://www.hyperledger.org/blog/2016/11/01/hyperledger-welcomes-iroha" \t "_blank), a way to incorporate the blockchain distributed ledger into business infrastructure projects, or [Hyperledger Sawtooth](https://www.hyperledger.org/projects/sawtooth" \t "_blank), a modular blockchain suite.

**[ To comment on this story, visit [Computerworld's Facebook page](https://www.facebook.com/Computerworld/posts/10155292052819680" \t "_blank). ]**

Last year, Intel proposed [its version of code for Sawtooth](https://software.intel.com/en-us/blogs/2017/02/14/the-second-coming-of-blockchain) called "Sawtooth Lake," a modular platform for building, deploying and running distributed ledgers, which it submitted to the Hyperledger blockchain project.

Another current project under Hyperledger is Burrow, a smart contract system built in part to the [Ethereum Virtual Machine](https://www.ethereum.org/" \t "_blank) specification - a block application platform.

Hyperledger Composer will offer developers a way to build smart contracts for multiple industries by sharing the components of Iroha, Sawtooth, Burrow or Fabric, according to Hyperledger Executive Director Brian Behlendorf.

For example, the blockchain ledger could enable automated contracts between insurance companies and beneficiaries, Behlendorf said. In such a blockchain smart contract, an insurance company could agree to pay a farmer if drought conditions persist during a season for a set period of time.

The contract's blockchain-based software script would then run across multiple server nodes to determine when a drought condition has been met and payment to the beneficiary is in order.

"It's a way to automate a lot of potential business processes," Behlendorf said.

Another example of a blockchain-enabled smart contract is the electronic documentation or bill of materials for shipping containers as they travel the world on seagoing vessels and railways. The current paper-based system involved in tracking shipments can account for up to half the cost of transport, according to Behlendorf.

Maersk

Ninety percent of goods in global trade are carried by the ocean shipping industry each year. A new blockchain solution from IBM and Maersk will help manage and track the paper trail of tens of millions of shipping containers across the world by digitizing the supply chain process.

"So if you can automate a lot of the documentation processes, you have a chance of cutting many of these costs, which the shipping industry is desperate for," Behlendorf said.

For example, IBM and Maersk, the world's largest container shipping operator, recently announced [they are piloting](https://www-03.ibm.com/press/us/en/pressrelease/51712.wss" \t "_blank) a blockchain-based, electronic distributed ledger using Hyperledger Fabric.

Smart contracts could also be used to automate the tracking of electronic healthcare records, so that healthcare providers could confirm patient consent each time they want to share the sensitive information between organizations.

"There are different implementations of different smart contract systems in each of these four frameworks, but there's the potential [with Composer] to weave these together," Behlendorf said.

# ComputerWorld

# 4 ways blockchain is the new business collaboration tool

## Smart contracts, healthcare data-sharing and microgrids are all taking advantage of the technology

[](http://www.computerworld.com/author/Lucas-Mearian/)By [Lucas Mearian](http://www.computerworld.com/author/Lucas-Mearian/)

Senior Reporter, Computerworld | May 23, 2017 3:01 AM PT



While [blockchain may have cut its teeth on the cryptocurrency Bitcoin](http://www.computerworld.com/article/3191077/security/faq-what-is-blockchain-and-how-can-it-help-business.html" \t "_blank), the distributed electronic ledger technology is quickly making inroads across a variety of industries.

That's mainly because of its innate security and its potential for improving systems  operations all while reducing costs and creating new revenue streams.

David Schatsky, a managing director at consultancy [Deloitte LLP](https://www2.deloitte.com/us/en.html" \t "_blank), believes blockchain's diversity speaks to its versatility in addressing business needs, but "the impact that blockchain will have on businesses in various industries is not yet fully understood."

This year, blockchain technology is expected to become a key business focus for many industries, according to [a Deloitte survey](https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-survey-blockchain-reaches-beyond-financial-services-with-some-industries-moving-faster.html" \t "_blank) conducted late last year.

The online survey of 308 blockchain-knowledgeable senior executives at organizations with $500 million or more in annual revenue found many placed it among their company's highest priorities. Thirty-six percent believe blockchain has the potential to improve systems operations, either by reducing costs or increasing speed, and 37% cited blockchain's superior security features as the main advantage. The remaining 24% say it has the potential to enable new business models and revenue streams.

Although 39% of senior executives at large U.S. companies had little or no knowledge about blockchain technology, the rest said their knowledge ranged from "broad to expert -- and 55% of that group said their company would be at a competitive disadvantage if it fails to adopt the technology.

The bottom line: both the understanding of and commitment to blockchain varies by industry. But most see it as disruptive.

"It is fair to say that industry is still confused to a degree about the potential for blockchain," David Schatsky, managing director of Deloitte LLP, said in a statement. "More than a quarter of surveyed knowledgeable execs say their companies view blockchain as a critical, top-five priority. But about a third consider the technology overhyped."

Those already embracing blockchain are finding a new independence in their ability to transmit both sensitive data and money securely, enabling a new business dynamic.

Blockchain is a decentralized electronic, encrypted ledger or database platform -- in other words, a way to immutably store digital data so that it can be securely shared across networks and users. As a peer-to-peer network, combined with a distributed time-stamping server, blockchain databases can be managed autonomously. There's no need for an administrator; the users are the administrator.

Blockchain eliminates huge amounts of recordkeeping, which can get confusing when there are multiple parties involved in a transaction, according to Saurabh Gupta, vice president of strategy at IT services company Genpact. "Blockchain and distributed ledgers may eventually be the method for integrating the entire commercial world's record keeping," he said.

#### Smart contracts

Blockchain distributed ledgers can be used to automatically execute business contracts. The peer-to-peer database first captures all terms and conditions between an organization and its customers, then uses data gleaned across distributed nodes or servers to determine when those conditions have been met and payment is authorized.

For example, an insurance company could pen a policy for farmers that states they will be paid if a drought affects agricultural production; the condition of the contract may statetcat if a drought persists for 30 days, payment is made. There is no need for human intervention in determining whether those drought conditions have been met and payments can proceed automatically, streamlining the process. The result: saved time and money.

In a similar way, blockchain-based smart contracts can be used to automatically execute payments between financial institutions.

Accenture recently released a report that claimed blockchain technology [could reduce infrastructure costs](https://newsroom.accenture.com/news/blockchain-technology-could-reduce-investment-banks-infrastructure-costs-by-30-percent-according-to-accenture-report.htm" \t "_blank) for eight of the world's 10 largest investment banks by an average of 30%, "translating to $8 billion to $12 billion in annual cost savings for those banks."

Payments, clearance and settlement in the financial services industry -- including stock markets -- is rife with inefficiencies because each organization in the process maintains its own data and must communicate with the others through electronic messaging about where it is in the process. Because of that, settlement typically takes two days. In turn, delays in settlements force banks to set aside money that could otherwise be invested.

With its ability to instantly share data with each organization involved in a blockchain database or ledger, the technology reduces or eliminates the need for reconciliation, confirmation and trade break analysis as key parts of a more efficient and effective clearance and settlement process, according to Accenture.

#### Enabling businesses to avoid transaction fees

Most payment systems are administered by financial institutions, such as banks. When money is transferred between businesses, there's typically a fee associated with it -- especially for small to mid-sized businesses.

Large enterprises have always enjoyed an advantage in the global market, be it the capital to absorb the cost of transfer fees (or getting lower fees), better intellectual property protection, and a host of other advantages that come with having more  capital and greater influence.

Blockchain technology helps level the playing field, enabling SMBs to compete in that global market.

For example, the [B2B payment service Veem](https://www.veem.com/our-story/" \t "_blank), leverages blockchain to allow its SMB customers to transfer funds internally for no fee; that compares to larger banks that charge around $50 per wire transaction.

Veem's CEO Marwan Forzley believes blockchain is an opportunity to "remove the middle man from international transactions, which directly impacts the experience of paying suppliers and contractors, the timing of these transactions and the fees that are directly impacting the SMBs bottom line."

#### Sharing patient data, ensuring doctors get paid

While electronic healthcare records (EHRs) have helped in the centralization of patient data to some extent, sharing that sensitive information with various healthcare providers, such as medical specialists, can be difficult at best because EHR platforms are not standardized across organizations.

Healthcare organizations could use the cryptographically secure, decentralized blockchain ledger to pre-authorize the sharing of a patient's information.

Last year, the MIT Media Lab and Beth Israel Deaconess Medical Center tested a proof-of-concept that shared information about patient medications through a blockchain ledger called MedRec. MedRec was based on the [Ethereum blockchain platform](https://www.ethereum.org/" \t "_blank) for smart contracts.

In their analysis paper, titled "[A Case Study for Blockchain in Healthcare](https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf" \t "_blank)," the MIT and Beth Israel Deaconess Medical Center researchers found blockchain "could contribute to secure, interoperable EHR systems."

In addition, healthcare IT vendors and the U.S. government are exploring blockchain's potential. Earlier this year, IBM's Watson Health artificial intelligence unit  signed a two-year joint-development agreement with the U.S. Food and Drug Administration (FDA) to explore using [blockchain technology to securely share patient data](http://www.computerworld.com/article/3156504/healthcare-it/ibm-watson-fda-to-explore-blockchain-for-secure-patient-data-exchange.html" \t "_blank) for medical research and other purposes.

IBM Watson Health and the FDA plan to explore the exchange of patient-level data from several sources, including electronic medical records (EMRs), clinical trials, genomic data and health data from mobile devices, wearables and the "Internet of Things." The initial focus will be on oncology-related information.

Healthcare is also hampered with an inefficient payment system, where insurance companies fight with providers.

"Insurance companies have already given prior approval based on medical necessity or preauthorization and I've got to fight collect it..., really?" said Gene Thomas, CIO of [Memorial Hospital](http://www.gulfportmemorial.com/mhg/home.aspx" \t "_blank), a 445-bed facility in Gulfport, Miss. "Depending on who you talk to, 17 cents, 21 cents... of every healthcare dollar is spent on collections. Are you kidding me?"

Underpinning a shared ledger where all parties involved in a healthcare insurance contract -- patient, provider and payer -- all see the same information at the same time, blockchain has the potential of smoothing out the "arduous, high cost, high friction process.

"Everyone's posting to the same thing, it's all transparent. I've got high hopes that if there's any place blockhchain could actually have an impact in healthcare, it's on [the] revenue cycle side," Thomas said.

In light of that need, Deloitte's report found that healthcare and life sciences have the most aggressive deployment plans for blockchain of any industry, with 35% of survey respondents indicating their organization plans to deploy blockchain within the next year.

#### Selling energy through microgrids

Because of blockchain, residents of the Park Slope area of Brooklyn are now able to sell power generated from rooftop solar panels via [a microgrid enabled by a blockchain ledger](http://www.computerworld.com/article/3191256/sustainable-it/blockchain-used-to-power-brooklyn-microgrid-for-solar-energy-re-sale.html" \t "_blank) that records every transaction made with a local utility.

The physical microgrid, set up by Siemens Digital Grid Division, includes network control systems, converters, lithium-ion battery storage and smart electric meters. In case of another hurricane like Sandy in 2012, residents on the microgrid would continue to have power for a time -- even during a blackout -- as they could switch  to battery reserves.

A microgrid is a form of distributed energy generation that can function independently from the traditional, centralized regional power grid; it can enable towns, small cities or corporations to develop their own energy sources and power storage systems (via lithium-ion or flow batteries), distribute that energy and even sell excess power back to local utilities.

The Brooklyn Microgrid blockchain database is a web-based bookkeeping system that uses cryptographic technology to save energy data in a way that is both inexpensive and forgery-proof, the companies said.

The Brooklyn Microgrid enables residents to sell energy back to the local utility -- a process known as "net metering" -- and it allows those without solar panels to purchase green power credits from their neighbors. The blockchain platform for the microgrid is enabled by Brooklyn-based energy startup LO3 Energy.

The same blockchain technology that allows residential solar power users to sell excess power back to utilities can do the same for businesses seeking to lower their electricity costs.

# New Co Shift

# Graphic: Blockchain for Every Industry



By Jeremiah Owyang and Jaimy Szymanski

Blockchain technology has the potential to upend the way every industry manages its information and data, not only financial services.

Imagine being able to track shipments through your supply chain with ease, down to the individual package or even component level. Or, executing a contract with a vendor without the need for an intermediary auditor. Blockchain can even help verify materials and food sourcing to ensure health and ethical standards are maintained.

Though most who are familiar with the technology equate it to Bitcoin, opportunities abound in other verticals in effectively storing transaction, customer, and supplier data in a transparent, unchangeable ledger online. Any relationship that depends on third-party maintenance, or those that require multiple data sources to fulfill customer expectations for cohesive experiences, can be improved by blockchain applications.

In the latest Crowd Companies market projection report, “The Business Models of Blockchain” ([available to our innovation council members only](http://crowdcompanies.com/" \t "_blank)), we explore how blockchain technology enables transparency and accountability of assets in every industry through shared, immutable ledgers. These impacts are outlined at a high level in the infographic above. ([Click here or on the image for the hi-res version to share with your networks.](http://crowdcompanies.com/blog/wp-content/uploads/2017/06/Blockchain-Beyond-Bitcoin_F_RGB_web.jpg" \t "_blank))

The potential industry disruptions included in the infographic are:

**Legal:** “Smart contracts” stored on the blockchain track contract parties, terms, transfer of ownership, and delivery of goods or services without the need for legal intervention.

**Supply Chain:** By utilizing a distributed ledger, companies within a supply chain gain transparency into shipment tracking, deliveries, and progress among other suppliers where no inherent trust exists.

**Government:** Blockchain offers promise as a technology to store personal identity information, criminal backgrounds, and “e-citizenship,” authorized by biometrics.

**Energy:** Decentralized energy transfer and distribution are possible via micro-transactions of data sent to blockchain, validated, and re-dispersed to the grid while securing payment to the submitter.

**Food:** Using blockchain to store food supply chain data offers enhanced traceability of product origin, batching, processing, expiration, storage temperatures, and shipping.

**Retail:** Secure P2P marketplaces can track P2P retail transactions, with product information, shipment, and bills of lading input on the blockchain, and payments made via Bitcoin.

**Healthcare:** Electronic medical records stored in a blockchain, accessed and updated via biometrics, allow for the democratization of patient data and alleviate the burden of transferring records among providers.

**Insurance:** When autonomous vehicles and other smart devices communicate status updates with insurance providers via the blockchain, premium costs decrease as the need for auditing and authenticating data vanishes.

**Travel and Hospitality:** Passengers store their authenticated “single travel ID” on the blockchain for use in lieu of travel documents, identification cards, loyalty program IDs, and payment data.

**Education:** Educational institutions could utilize the blockchain to store credentialing data around assessments, degrees, and transcripts.

As part of our research coverage on disruptive technologies at [Crowd Companies](http://crowdcompanies.com" \t "_blank), blockchain aligns with our prior research on the Collaborative Economy, where technologies strengthen P2P relationships to bypass central institutions. Additionally, blockchain technologies will be harnessed by autonomous technologies, enabling machine-to-machine transactions.