Blockchain Techology

What is blockchain? The complete guide

The much-hyped distributed ledger technology (DLT) has the potential to eliminate huge amounts of record-keeping, save money, streamline supply chains and disrupt IT in ways not seen since the internet arrived.

By Lucas Mearian

Senior Reporter, Computerworld | 30 JANUARY 2019 11:13 AEDT

Blockchain, which began to emerge as a real-world tech option in 2016 and 2017, is poised to change IT in much the same way open-source software did a quarter century ago. And in the same way Linux took more than a decade to become a cornerstone in modern application development, Blockchain will likely take years to become a lower cost, more efficient way to share information and data between open and private business networks.

Based on a peer-to-peer (P2P) topology, blockchain is a distributed ledger technology (DLT) that allows data to be stored globally on thousands of servers – while letting anyone on the network see everyone else's entries in near real-time. That makes it difficult for one user to gain control of, or game, the network.

However, in highly publicized incidents over the five years, blockchains *have* been hacked, typically through a cryptocurrency application such as bitcoin. Smaller blockchains with fewer nodes (or computers) have also been susceptible to fraud, with would-be thieves gaining control of the majority of nodes.

For businesses, however, blockchain holds the promise of transactional transparency – the ability to create secure, real-time communication networks with partners around the globe to support everything from supply chains to payment networks to real estate deals and healthcare data sharing.

Recent hype around this relatively new technology is real because DLT, in essense, represents a new paradigm for how information is shared; tech vendors and enterprises, not surprisingly have rushed to learn how they can use the distributed ledger technology (DLT) to save time and admin costs. Numerous companies have already rolled out, or are planning to launch, pilot programs and real-world projects across a variety of industries - everything from financial technology (FinTech) and healthcare to mobile payments and global shipping.

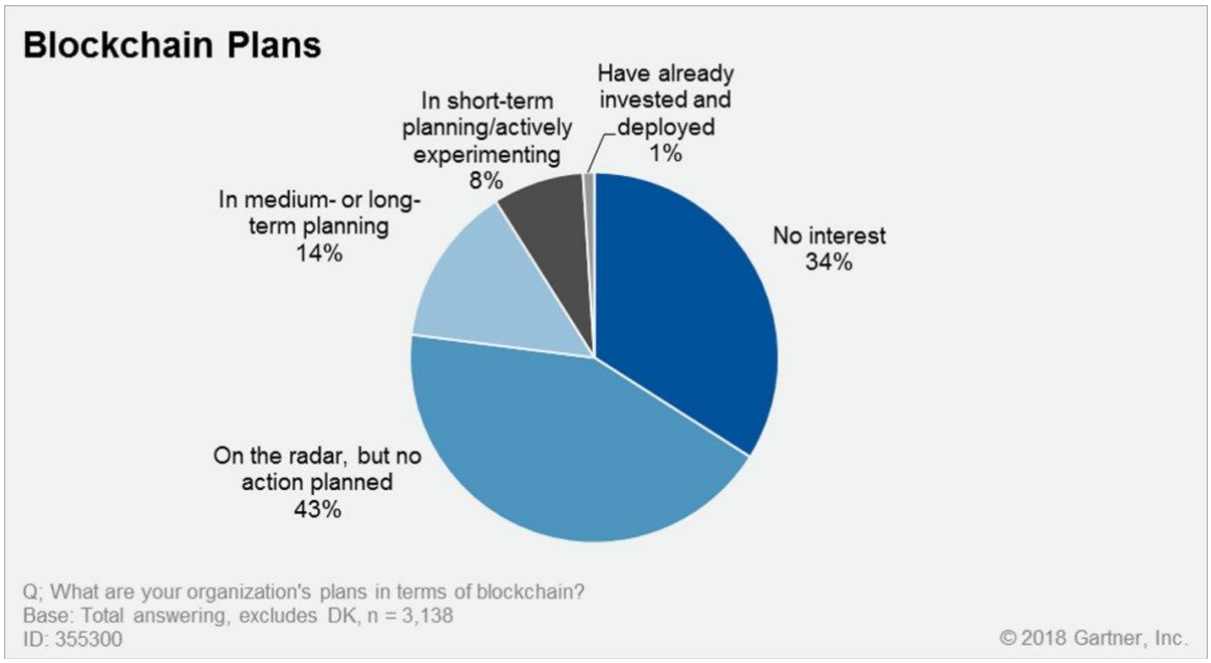
So while blockchain isn't going to replace traditional corporate relational databases, it does open new doors for the movement and storage of transactional data inside and outside of global enterprises.

Driven mainly by financial technology (fintech) investments, blockchain has seen a fast uptick in adoption for application development and pilot tests in a number of industries and will generate more than $10.6 billion in revenue by 2023, according

to a report from ABI Research. Most of that revenue figure is expected to come from software sales and services.

Blockchain adoption is expected be steady, as the changes it brings gain momentum, according Karim Lakhani, a principal investigator of the Crowd Innovation Lab and NASA Tournament Lab at the Harvard Institute for Quantitative Social Science. "Conceptionally, this is TCP/IP applied to the world of business and transactions," Lakhani said. "In the '70s and '80s, TCP/IP was not imaginable to be as robust and scalable as it was. Now, we know that TCP/IP allows us all this modern functionality that we take for granted on the web.

"Blockchain has the same potential."



Gartner

A Gartner survey of CIOs last spring revealed only 1% had blockchain deployed in production environments; that number has grown to 3.3% today, according to Gartner Distinguished Analyst Avivah Litan.

Martha Bennett, a principal analyst for Forrester Research, noted any blockchain or "DLT" project is a long-term strategic initiative, and disappointment is inevitable "when the hoped-for miracles fail to materialize.

"It's not realistic to expect a solid cost model or definitive benefits statement because it's simply too early for that," Bennett said. "To assemble real evidence, we need to have a number of fully operationalized, scaled-out deployments running for at least a couple of years. And we're simply not there yet."

TABLE OF CONTENTS

SHOW MORE

What is blockchain and how does it work?

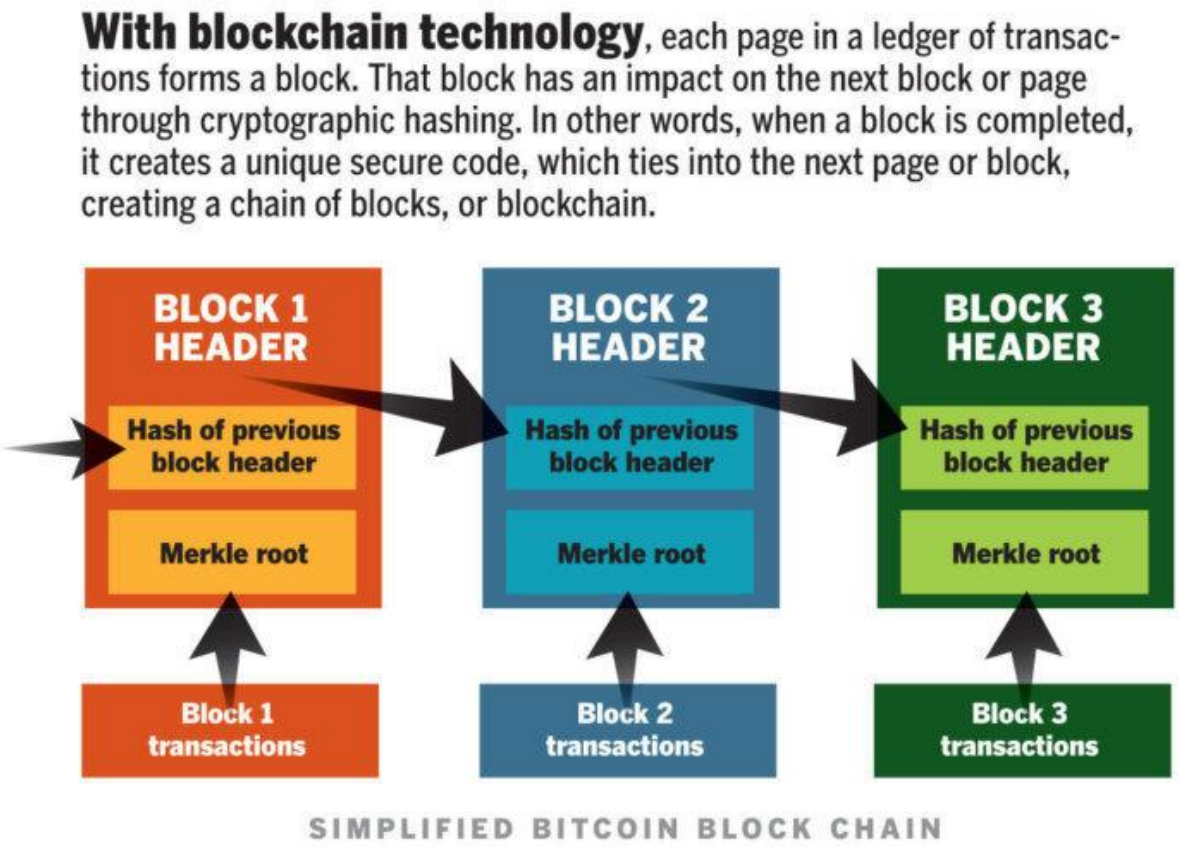
First and foremost, blockchain is a public electronic ledger built around a P2P system that can be openly shared among disparate users to create an unchangeable record of transactions, each time-stamped and linked to the previous one. Every time a set of transactions is added, that data becomes another block in the chain (hence, the name).

Blockchain can only be updated by consensus between participants in the system, and once new data is entered it can never be erased. It is a write-once, append-many technology, making it a verifiable and auditable record of each and every transaction.

While it has great potential, blockchain technology development is still early days; CIOs and their business counterparts should expect setbacks in deploying the technology, including the real possibility of serious bugs in the software used atop blockchain. And as some companies have already discovered, it's not the be-all solution to many tech problems.

Blockchain standards organizations, universities and start-ups have proposed newer consensus protocols and methods for spreading out the computational and data storage workload to enable greater transactional throughput and overall scalability – a persistent problem for blockchain. And the Linux Foundation's Hyperledger Project has created modular tools for building out blockchain collaboration networks.

While some industry groups are working toward standardizing versions of blockchain software, there are also hundreds of startups working on their own versions of the distributed ledger technology.



IDG

Each digital record or transaction in the electronic ledger is called a block. When a block is completed, it creates a unique secure code that ties it to the next block.

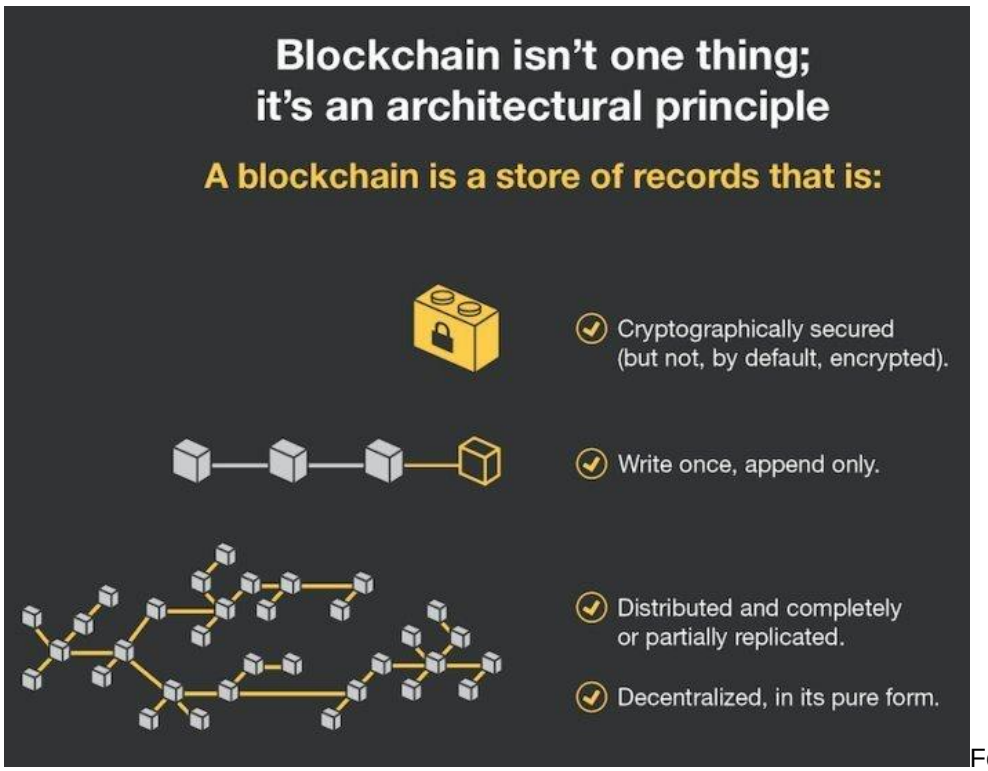
Why has blockchain been getting so much buzz? In a word, bitcoin – the wildly hyped cryptocurrency that allows for payment transcations over an open network using encryption and without exposing the identities of individual bitcoin owners. It was the first ever decentralized one when it was created in 2009. Other forms of cryptocurrency or virtual money, such as Ether (based on the Ethereum blockchain application platform), have also gained significant traction and opened new venues for cross-border monetary exchanges. (Ethereum was introduced in 2013 by developer Vitalik Buterin, who was 19 at the time.)

The term bitcoin was first... well, coined in 2008 when Satoshi Nakamoto (likely a pseudonym for one or more developers) wrote a paper 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."

For more than a year, however, Bitcoin has been on a roller coaster ride, with its value dropping from a peak of nearly $20,000 to a little more than $3,500, mainly due to the fact that it has no intrinsic value; its worth is based only on high demand and limited supply. Unlike fiat currencies or stocks, there is no institution or government backing the value of bitcoin.

That may change for cryptocurrencies someday.

Governments have already made overtures toward creating stablecoins, or cryptocurrency that's backed by a stable asset such a gold or traditional fiat currency. Blockchain is also being used to digitize other assets, such as cars, real estate and even artwork.



Forrester Research

Blockchain, or distributed ledger technology, isn't a single technology. Rather it's an architecture that allows disparate users to make transactions and then creates an unchangeable, secure record of those transactions.

Public vs. private blockchains

As a peer-to-peer network, combined with a distributed time-stamping server, public blockchain ledgers can be managed autonomously to exchange information between parties. There's no need for an administrator. In effect, the blockchain users are the administrator.

A second form of blockchain, known as private or permissioned blockchain, allows companies to create and centrally administer their own transactional networks that can be used inter- or intra-company with partners.

Additionally, blockchain networks can be used for "smart contracts," or scripts for business automation that execute when certain contractual conditions are met. For example, after a bad batch of lettuce resulted in customers becoming sick from e-coli, Walmart and IBM created a blockchain-based supply chain to track produce from farm to table. Walmart has asked its produce suppliers to input their data to the blockchain database by September 2019. Once on the blockchain, produce can be automatically tracked through smart contracts from point to point, removing human intervention and error.

IBM

After piloting a blockchain-based produce supply chain tracking system, Walmart and Sam's Club are telling suppliers to get their product data into the system so they can begin tracking produce from farm to store. The deadline: September 2019.

De Beers,which controls about 35% of the world's diamond production, has also launched a blockchain-based supply chain to track diamonds for authenticity and to help ensure they aren't coming from war-torn regions where miners are exploited.

Smart contracts can also be used to approve the transfer of assets, such as real estate. Once conditions are met between buyers, sellers and their financial institutions, property sales can be confirmed on DLT. For example, New York-based ShelterZoom this year is launching a real estate mobile application that lets real estate agents and clients see all offers and acceptances in real time online. It will also allow access to property titles, mortgages, legal and home inspection documents through the Ethereum-based encrypted blockchain ledger.

TrustChain

The De Beers's TrustChain blockchain network will track and authenticate diamonds, precious metals and jewelry at all stages of the global supply chain, from the mine to the retailer.

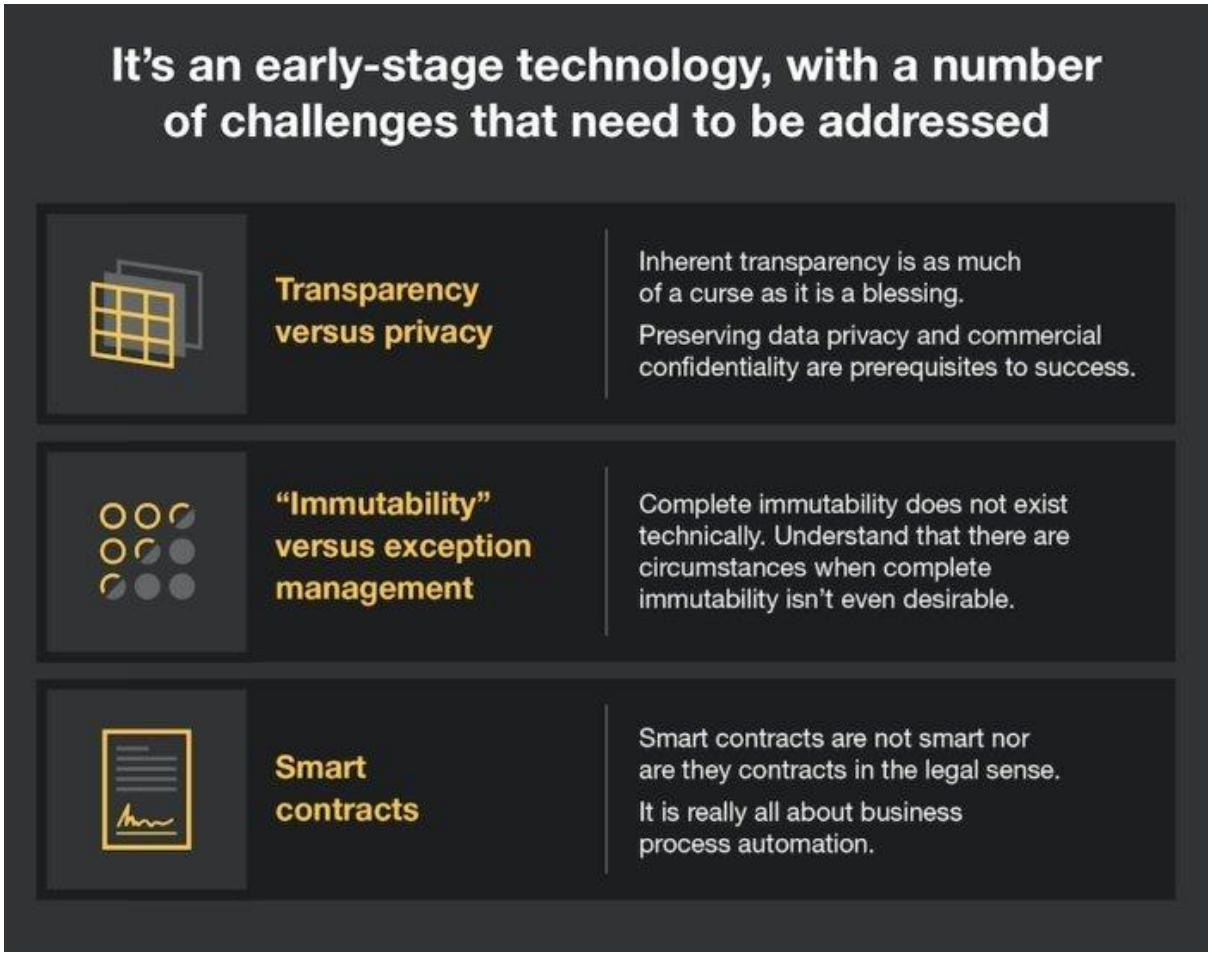
How secure is blockchain

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

"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," Tapscott said. "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.

"So again, [it's] not un-hackable, but significantly better than anything we've come up with today," he said.

The computing resources needed for most blockchains are tremendous, Tapscott said, because of the number of computers involved. For example, the bitcoin blockchain harnesses anywhere between 10 and 100 times as much computing power as all of Google's serving farms put together.

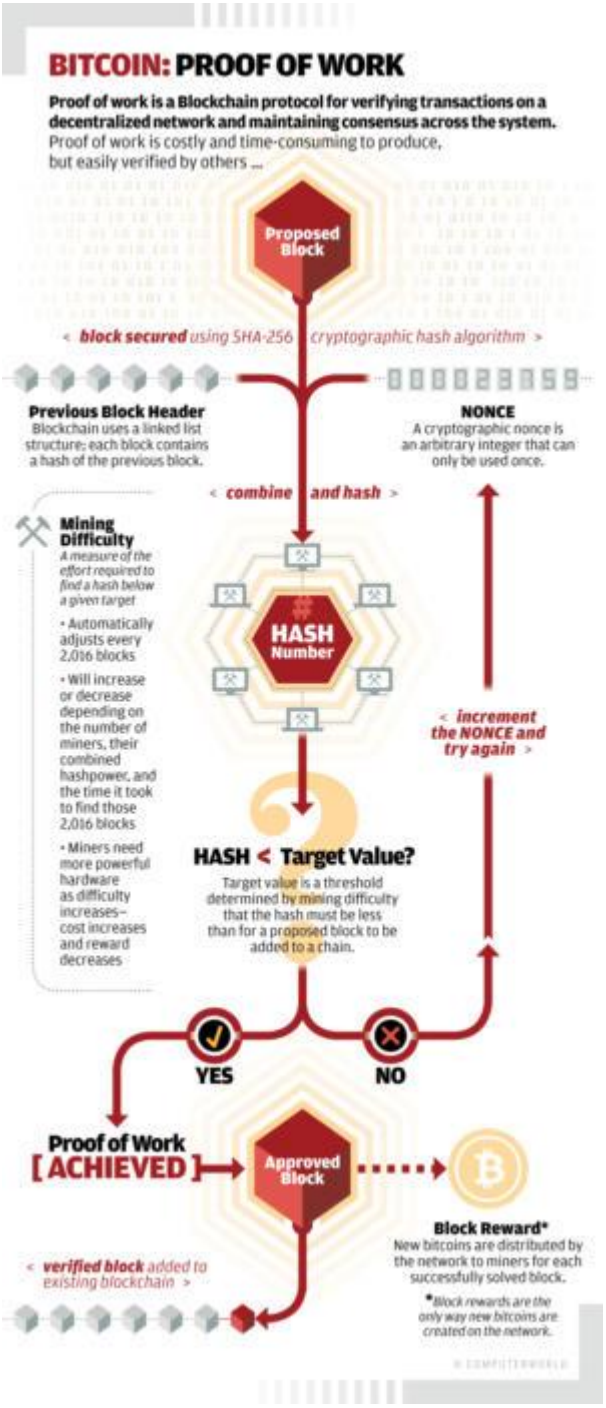


Forrester Research

As with any emerging technology, blockchain faces challenges and barriers to adoption.

But even a larger scale can't always prevent hacks.

A recent “51 percent attack” on the Ethereum Classic token exchange showed why even blockchain is not impermeable to gaming. A 51 percent attack refers to a bad actor who gains control of the majority of CPUs in a cryptocurrency mining pool. Such attacks are generally limited to smaller blockchains with fewer nodes because they're more susceptible to a single person seizing control based on a Proof of Work (PoW) consensus mechanism.



Computerworld / IDG

Even though blockchain networks are secure, the applications running atop them may not be as safe, according to Bruce Schneier, a cryptographer and security expert.

"That's not how this sort of thing will get broken. It'll get broken because of some insecurity in the software," Schneier said.

Blockchain's advances rely on scalablity

One of the major issues facing blockchain involves scalability, or its ability to complete transactions in near real time, such as clearing payments via credit cards.

Scalability has already been identified as an issue with cryptocurrencies such as bitcoin and Ethereum's Ether. If a distributed ledger is to achieve adoption by financial technology (FinTech) companies and compete with payment networks hundreds of times faster, it must find a way to boost scalability and throughput and address latency problems.

Enter "sharding."

Sharding is one of several popular methods being explored by developers to increase transactional throughput. Simply stated, sharding is a way of partitioning to spread out the computational and storage workload across a P2P network so that each node isn't responsible for processing the entire network's transactional load. Instead, each node only maintains information related to its partition, or shard.

The information contained in a shard can still be shared among other nodes, which keeps the ledger decentralized and theoretically secure because everyone can still see all ledger entries; they simply don't process and store all of the information such as account balances and contract code, for instance.

In today's blockchains, each authenticating computer or node records *all* the data on the electronic ledger and is part of the consensus process. In large blockchains such as bitcoin, the majority of participating nodes must authenticate new transactions and record that information if they are to be added to the ledger; that makes completing each transaction slow and arduous.

Because of that, bitcoin, which is based on a PoW, can only process 3.3 to 7 transactions per second – and a single transaction can take 10 minutes to finalize.

Ethereum, another popular blockchain ledger and cryptocurrency, is only able to process from 12 to 30 transactions per second. By comparison, Visa's VisaNet on average processes 1,700 transactions per

Last year, Ethereum began exploring ways to increase performance after the blockchain ledger and cryptocurrency reached more than one million transactions per day.

Ethereum settled on two proposed fixes. One was a "layer 2" mechanism – processing transactions off the chain in a standard database and only recording permanent entries on the ledger; the other solution was sharding, allowing many more transactions to be processed in parallel at the same time.

Blockchain standards organizations and startups are also exploring newer consensus mechanisms to create more efficient and less compute intensive DLT.

Which industries use blockchain?

Even as those advances are being explored, industries are ramping up pilots and live deployments of blockchain. Shipping. Fintech. Healthcare, Energy and Real Estate. Blockchains are being put to a wide variety of uses in a myriad of vertical industries. (It's even been touted as a way to exchange carbon credits.)

In shipping, for example, a bill of lading for cargo shipments has traditionally been paper based, which requires multiple sign-offs by inspectors and receivers before

goods can be delivered. Even when the system is electronic, it still requires multiple parties to sign off on cargo shipments, creating a lengthy administrative process.

Maersk is piloting a blockchain-based cargo tracking system with 94 partner participants, including more than 20 port and terminal operators; smart contract technology can track the temperature of containers using IoT technology and report on when they leave ports and reach destinations.

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.

IBM, Maersk

Each participant in the shipping supply chain can view the progress of goods through the blockchain ledger, understanding where a container is in transit. They can also see the status of customs documents, or view bills of lading and other data in real time. And, because it's an immutable record, no one party can modify, delete or even append any one of the blocks without the consensus from others on the network.

"Blockchain and distributed ledgers may eventually be the method for integrating the entire commercial world's record keeping," said Saurabh Gupta, vice president of strategy at IT services company Genpact.

Blockchain eliminates huge amounts of recordkeeping, which can get confusing when there are multiple parties involved in a transaction.

Genpact, for example, announced a service 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.

Blockchain in FinTech

But it's financial services technology where blockchain is currently shining brightly.

At a high level, blockchain removes third parties from the equation; in other words, a financial transaction on a blockchain needs no bank or government backer, and that means no fees.

Blockchain lends itself to a number of common use cases in the financial services market, including regulatory compliance, cross-border payments & settlements,

custody and asset tracking, and trade finance and post-trade/transaction settlements, according to IDC.

Because blockchain entries can be seen in real time, the technology also has the potential to reduce time for clearance and settlement, which can take up to five days.

One Accenture report 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."

In the case of cross-border payments, processing is often complex and includes multiple layers of communication among payment participants to verify transactions – an operation known as payment and settlement.

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. As a result, settlements typically take two days. Those delays in settlements force banks to set aside money that could otherwise be invested.

Because it can instantly share data with blockchain users, the technology reduces or eliminates the need for reconciliation, confirmation and trade break analysis. That helps yield a more efficient and effective clearance and settlement process, according to Accenture.

J.P. Morgan has created what is arguably one of the largest blockchain payments networks to date: the Interbank Information Network (IIN). The financial services company announced in late 2017 that the Royal Bank of Canada and Australia and New Zealand Banking Group Ltd. had joined INN, "representing significant cross-border payment volumes."

J.P. Morgan created the network to significantly reduce the number of participants needed to respond to compliance and other data-related inquiries that can delay payments.

"IIN will enhance the client experience, decreasing the amount of time – from weeks to hours – and costs associated with resolving payment delays," said Emma Loftus, Head of Global Payments and FX at J.P. Morgan Treasury Services. "Blockchain capabilities have allowed us to rethink how critical information can be sourced and exchanged between global banks."

Mastercard, meanwhile, in late 2017 also launched its own blockchain network to enable partner banks and merchants to make cross-border payments faster and more securely. The Mastercard blockchain service can be used to clear credit card transactions and eliminate administration tasks using smart contract rules, thus, speeding up transaction settlement.

Blockchain and mobile payments

Prior to rolling out a blockchain-based electronic exchange, peer-to-peer foreign exchange provider KlickEx was limited in scale by the company's own infrastructure;

it served about 1 million users per day across eight countries, or about 80% of households in its Pacific region.

Today, the monetary exchange handles about 90% to 95% of all electronic payments for the region that are for $200 or less. When not overtaxed, the old KlickEx exchange system was able to clear payments in between 90 and 200 seconds. But a common processing issue often slowed the process: payments received would outpace payments issued, forcing the exchange to use batch processing. That caused payments to enter queues and created a delay that could take days.

A new blockchain-based payment system that KlickEx has created can process cross-border payments in seconds.

IBM/KlickEx

KlickEx Group, a United Nations-funded, Pacific-region financial services company, and Stellar.org, a nonprofit organization that supports an open-source blockchain network for financial services, are backing a new cross-border, mobile payments service. This is an example of the iOS app.

The Polynesian payments system provider partnered with IBM to create an open-source payment network as a new international exchange based on a blockchain electronic ledger. The new network uses IBM's Blockchain Platform, a cloud service, to enable the electronic exchange of 12 different currencies across Pacific Islands as well as in Australia, New Zealand and the United Kingdom.

"In bringing IBM in to mature the technology, we think we're pushing something like 8 million...payments per day capacity, which is a long way up from where we started," KlickEx CEO Robert Bell said. "So the new real-time system based on blockchain means payment happens immediately, rather than in batch files."

Blockchain for healthcare

Blockchain can also act as a collaboration network, enabling varying parties to exchange and add to information, such as a patient's electronic healthcare record, in real time. The blockchain acts as a verification tool, ensuring only authorized users — such as a physician, insurance provider or patient — can make changes to the ledger.

Blockchain's interoperability could underpin data exchange, serving as an alternative to today's health information exchanges (HIEs); essentially, it would act as a mesh network for transmitting secure, near real-time patient data for healthcare providers, pharmacies, insurance payers and clinical researchers, according to IDC.

In 2017, startup MintHealth, launched a portable, personal health record for mobile based on a blockchain exchange. MintHealth will be rolling out the platform to commercial health insurance plans to help patients with chronic conditions such as heart failure, diabetes and hypertension that account for more than 90% of healthcare costs today. In addition, patients at risk for, but not yet suffering from, chronic conditions will also benefit by having access to their medical records and control of their own health data by entering data such as vital signs or blood glucose levels.

Start-up Hu-manity.co has partnered with IBM to develop an electronic ledger that gives consumers the cryptographic key to grant to their personal data, even allowing patients or others to control the specific purpose for which it's used, while also allowing them to eventually profit from it.

The new Global Consent Ledger will initially begin with healthcare data from U.S. residents and provide a digital data trail stored on the IBM Blockchain Platform, which uses the Hyperledger Fabric specification.

Hu-manity.co

Hu-manity's title of ownership for personal data, which also includes a blockchain protected hash key.

IBM Watson Health and the U.S. Food and Drug Administration are also exploring the use of blockchain for secure patient data exchange, including sensitive electronic

medical records (EMRs), clinical trials and data culled from mobile devices and wearables.

In November, Amazon announced an analytics service aimed at scouring unstructured data within EMRs to offer insights that physicians can use to better treat patients. Amazon's new Comprehend Medical AWS cloud service is a natural-language processing engine that purports to be able to read physician notes, patient prescriptions, audio interview transcripts, and pathology and radiology reports – and use machine learning algorithms to spit out relevant medical information to healthcare providers.

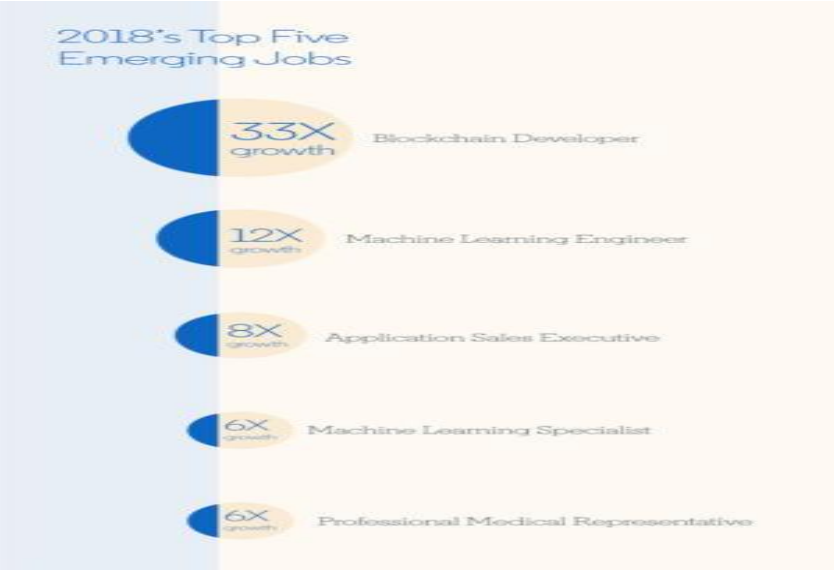
And in early 2019, SAP launched a supply chain tracking service based on blockchain that will enable drug wholesalers to authenticate drug packaging returned from hospitals and pharmacies.

SAP's Information Collaboration Hub for Life Sciences will initially be used to trace the return of unused drugs to wholesalers. But SAP plans to expand use of the technology to include a broader range of pharmaceutical supply chain processes.

Blockchain careers are taking flight

As more businesses explore blockchain pilots, jobs for Blockchain developers are becoming a premium. Blockchain developer is ranked first among the top five emerging careers, and job postings for workers with those skills have more than doubled this year.

In short, demand for blockchain professionals is skyrocketing.

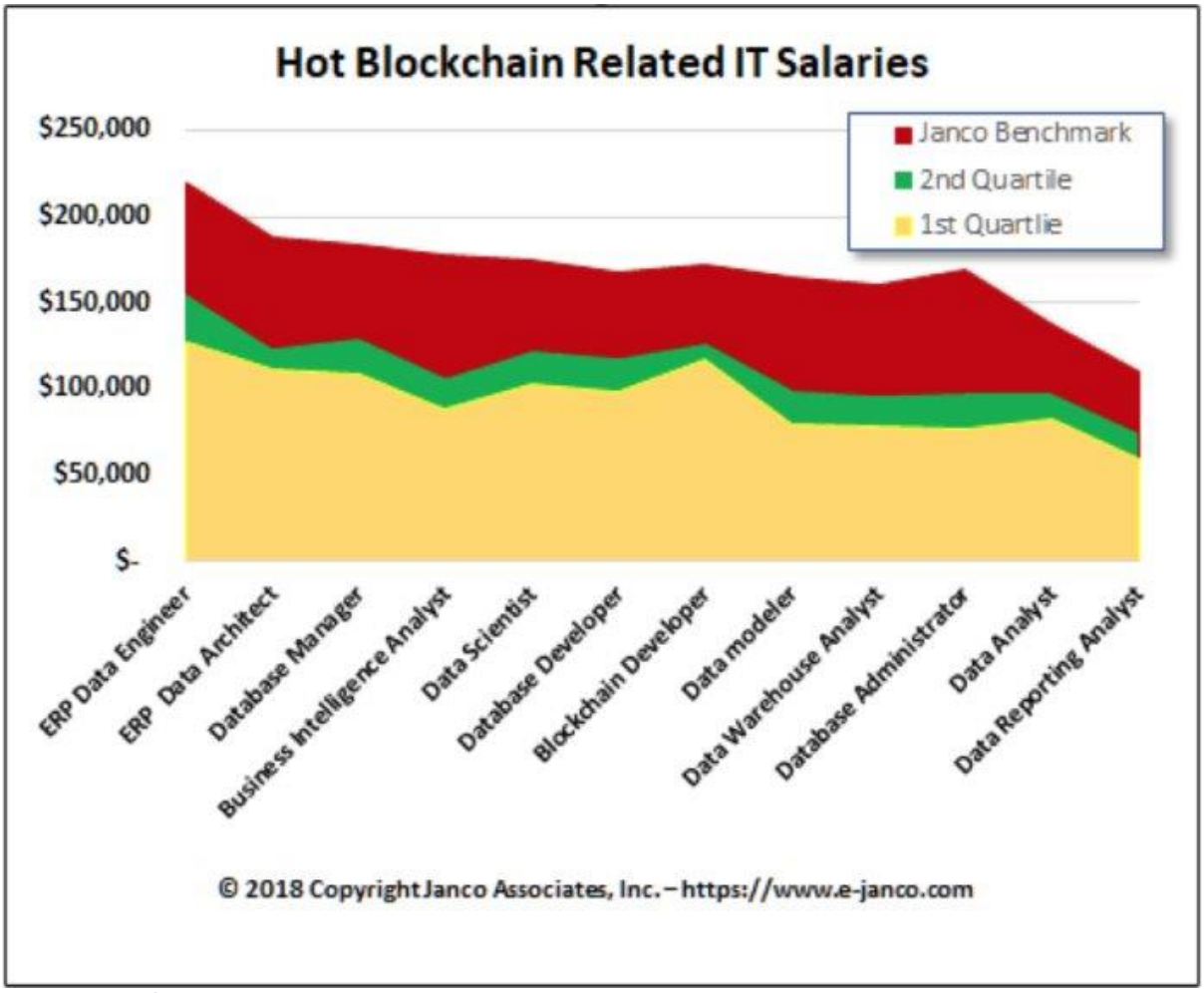


LinkedIn

In December, LinkedIn revealed its top five emerging careers and – in concert with other recent data – found that blockchain developer is at the top of the list.

Job listings for those who can create blockchains have grown 33-fold in the past year, according to LinkedIn's 2018 U.S. Emerging Jobs Report. In distant second place are machine learning engineers.

Topcoder, a company that creates computer programming contests, announced its new Blockchain Community with partner ConsenSys. The community aims to teach programmers and engineers how to build blockchain applications.



Janco Associates

How companies should approach blockchain

Regardless of who developed any new technology, businesses should always take a pragmatic approach when adopting it. That's true of blockchain.

"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.

A growing number of blockchain distributed ledger platforms are now being developed in parallel, with specialized applications on top of them, according to Gupta. The industry will need further 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."

According to Angus Champion de Crespigny, Ernst & Young's Blockchain Leader, blockchain distributed ledger technology is also well suited to propagate security policies and identity access management, which can traverse a myriad of markets. 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 data cannot be modified. That makes it perfect for record keeping and auditing purposes, he added.

De Crespigny noted that more vendors are now producing business-specific products, "which is really what's needed."

Blockchain: Too much hype?

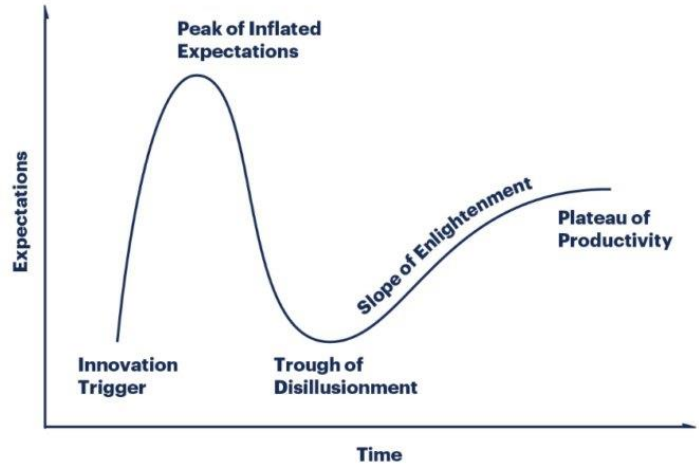
In a joint report released in late 2018 for the Monitoring, Evaluation, Research and Learning (MERL) Technology conference, researchers studied 43 blockchain use cases and concluded that all underdelivered on claims.

And, when they reached out to several blockchain providers about project results, the silence was deafening. "Not one was willing to share data," the researchers said in their blog post.

In their research, Christine Murphy, a social researcher at Social Solutions International and John Burg and Jean Paul Pétraud, fellows at the U.S. Agency for International Development, found a proliferation of press releases, white papers and persuasively written articles touting the many attributes of blockchain.

"However, we found no documentation or evidence of the results blockchain was purported to have achieved in these claims. We also did not find lessons learned or practical insights, as are available for other technologies in development," the researchers reported.

Avivah Litan, a Gartner vice president and distinguished analyst, said while the report's findings came as no surprise to her, it lacked balance. The researchers did not bother to ask why projects had not delivered on goals, such as improving transactional efficiency, transparency and privacy, she said.



Gartner

Garner's Hype Cycle for new technolgies. Distributed ledger technology or blockchain has been overhyped for years, but as enterprises deploy more pilots and business leaders in general become more familiar with it, it is heading into the Trough of Disillusionment and is expected to emerge on the slope of elightenment, according to Gartner.

"Back in early 2018, we'd already said... 99% of enterprise projects are dead end; 99% don't need the technology; they don't get out of the lab. They're a result of CEOs fear of missing out – the FOMO phenomenon," Litan said. "Having said all that, it's a very valuable technology. People started trying to use it before it was ready for prime time. That's true in the cryptocurrency world and in the enterprise blockchain world."

The future of blockchain

The reason some organizations feel angst about moving forward (or failing to do so) is because blockchain goes to the heart of how we organize our information and our records-keeping infrastructure, according to Lakhani. Any blockchain-centric overhaul is not going to happen overnight.

In the case of TCP/IP – the basis of the internet world that we now take for granted – it took 30 years to develop.

"When we started this in the 1970s, no one anticipated I could be in Boston and FaceTime with my mobile device with someone in Shanghai. That was science fiction," Harvard's Lakhani said.

"My sense is this will again take time. We need both business logic and technical logic to be figured out, the applications to be developed and people to be trained to use it," he said. "then we'll adapt our institutions to the new way of sharing information."

Senior Reporter Lucas Mearian covers financial services IT (including blockchain), healthcare IT and enterprise mobile issues (including mobility management, security, hardware and apps).